

MASTER THESIS:  
**Decoupling Theorems**

Oleg Szehr

Supervisors:

Marco Tomamichel, Frédéric Dupuis  
and Renato Renner

Institut für Theoretische Physik  
ETH Zürich, January 2011

## Acknowledgements

I thank Marco Tomamichel, Frédéric Dupuis and Renato Renner for the supervision of this project.

# Abstract

Decoupling theorems have proven useful in various applications in the area of quantum information theory. This thesis builds upon preceding work by Frédéric Dupuis [5], where a general decoupling theorem is obtained and its implications for quantum coding theory are studied. At first we generalize this theorem to the case where the average is taken over an approximate unitary 2-design. The second part of this thesis tackles the question whether or not it is possible to decorrelate CQ-states with classical operations. We obtain results similar to the pivotal Leftover Hash Lemma. Finally we analyze the decoupling power of permutation operators in a fully quantum context and show a general procedure that yields decoupling theorems with permutations.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Overview . . . . .	1
1.2	Notation and a glance at quantum mechanics . . . . .	3
1.3	Induced neighborhoods and the smoothed conditional min-entropy . .	8
<b>2</b>	<b>Decoupling via the Schatten 2-norm</b>	<b>9</b>
2.1	Lemma: Decoupling with the Schatten 2-norm . . . . .	9
2.2	An alternative proof of the decoupling theorem . . . . .	13
2.3	An improved bound for the decoupling theorem . . . . .	16
<b>3</b>	<b>Decoupling with almost 2-designs</b>	<b>19</b>
3.1	Unitary 2-designs . . . . .	20
3.2	Random quantum circuits . . . . .	21
3.3	Unitary almost 2-designs . . . . .	22
3.4	Decoupling with almost 2-designs . . . . .	24
3.5	Analysis of the decoupling formula . . . . .	32
<b>4</b>	<b>A smoothed version of the decoupling formula for <math>\varepsilon</math>-almost 2-designs</b>	<b>34</b>
<b>5</b>	<b>A classical analogue of the decoupling formula</b>	<b>40</b>
5.1	A “classicalized” Decoupling Lemma . . . . .	41
5.1.1	Counting permutation operators . . . . .	43
5.1.2	Action of twofold tensor products of permutation operators on a CQ-decoupling state. . . . .	45
5.1.3	Proof of the Decoupling Lemma for CQ-states . . . . .	47
5.2	A “Hash Lemma” like result . . . . .	49
5.3	A decoupling theorem for CQ-states and TPCP maps . . . . .	50
5.4	A decoupling theorem for CQ-states . . . . .	52

<b>6</b>	<b>Decoupling with 2-wise almost independent families of permutations</b>	<b>54</b>
6.1	Almost independent families of permutations . . . . .	54
6.1.1	Proving the equivalence of the two different views on almost independent families of permutations . . . . .	56
6.1.2	An exemplary pairwise independent family of permutations . .	60
6.2	CQ-decoupling theorem for pairwise $\varepsilon$ -dependent families of permuta- tions . . . . .	61
<b>7</b>	<b>Decoupling Quantum States with Permutation Operators</b>	<b>65</b>
7.1	The general setup . . . . .	65
7.2	The mathematical backbone for decoupling theorems with permutations	67
7.2.1	Basics from representation theory . . . . .	67
7.2.2	The structure of the commutant . . . . .	71
7.2.3	The dimension of $\text{Com}(R)^\dagger$ . . . . .	72
7.2.4	A basis for $\text{Com}(R)^\dagger$ . . . . .	76
7.2.5	Evaluating the term $\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2}$ . . . . .	78
7.3	Distance from classicality . . . . .	79
7.4	Decoupling with permutations operators . . . . .	84
7.5	Decoupling Quantum States with a Permutations followed by the Par- tial Trace . . . . .	86
<b>A</b>	<b>Hölder Inequality</b>	<b>92</b>
<b>B</b>	<b>Jensen Inequality</b>	<b>93</b>
<b>C</b>	<b>Swap Trick</b>	<b>94</b>
<b>D</b>	<b>The Murnaghan-Nakayama Rule</b>	<b>95</b>
D.1	The Irreps of $R$ . . . . .	96
	<b>Bibliography</b>	<b>100</b>

# Chapter 1

## Introduction

### 1.1 Overview

Quantum mechanical correlations are at the core of Quantum Information Theory. Correlated systems behave in a predictable way, such that the probability distributions obtained from measuring some observable on the one system partially determine possible measurement outcomes of the other. Knowledge about the physical state of one system implies knowledge about the state of any system correlated to it and correlations can be thought of as the carrier of quantum mechanical information. It is a basic issue in information theory to examine the correlations between different systems, since it includes the question of how much information one physical system contains over the other. The fact that two quantum systems are (almost) uncorrelated has significant consequences not only for information processing tasks but also for the physical behavior of these systems. In particular, this fact can be used to show that other systems are strongly correlated, which bonds the behavior of the one system to the other. Thus, a theorem that states conditions under which different systems are close to being uncorrelated provides substantial insight to the information theory of those and other systems. In [5] a very general decoupling theorem is derived (in the sequel called the Decoupling Theorem) and its impact on the theory of quantum coding is studied. Roughly speaking, the theorem applies in a situation where a joint system  $AR$  with possible correlations between the subsystems is given and a unitary evolution followed by an arbitrary physical process take place on the  $A$  part of the whole system. It provides a bound on how far a typical resulting state is from a completely uncorrelated state. Denoting the state of the system  $AR$  with  $\rho_{AR}$ , the unitary evolution with  $U_A$ , and the arbitrary physical process following the

unitary evolution with  $\mathcal{T}$ , the theorem states that

$$\int_{\mathbf{U}(A)} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R) \rho_{AR} (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\| dU \leq 2^{-\frac{1}{2}H_{\min}(A|E)_\omega - \frac{1}{2}H_{\min}(A|R)_\rho}.$$

The integration goes over the whole group of unitary matrices and is with respect to the normalized Haar measure. A quantum state with tensor product structure as  $\omega_E \otimes \rho_R$  in Quantum Mechanics represents a joint system whose subsystem are not correlated. The Decoupling Theorem bounds the average distance of the state  $\mathcal{T}((U_A \otimes \mathbb{1}_R) \rho_{AR} (U_A^\dagger \otimes \mathbb{1}_R))$  from a tensor product state. The right hand side of the above inequality is given in terms of the conditional  $H_{\min}$ -entropy, which is a prevalent measure of uncertainty. The term  $H_{\min}(A|R)_\rho$  for instance quantifies the uncertainty an observer with access to the  $R$  subsystem of  $AR$  has about the state of  $A$ .

Though stated in the context of coding theory, this theorem has far reaching implications in various areas of theoretical physics. Among other things, decoupling arguments and corollaries of the Decoupling Theorem deepened the insight into thermodynamics [4] and Black Hole Information theory [9]. Nevertheless, it turns out that for physical systems taking the average over all unitary matrices as it is done in the statement of the theorem is too strong an assumption. In a real system the internal dynamics are governed by the laws of nature and typically these very laws restrict the possible unitary evolutions of the system. One cannot expect that such dynamics produce arbitrary unitaries evenly distributed according to the Haar measure. Instead it was recently shown [7] that in a many qubit system with random local two-particle interactions the possible evolutions of the system constitute a unitary  $\varepsilon$ -almost 2-design.

This thesis discusses several decoupling results. The first chapter introduces the notation used and gives a brief overview of the quantum mechanical background. In the second chapter an alternative proof of the Decoupling Theorem resulting in a slightly tighter bound (as compared to [5]) is shown. The following two chapters are devoted to a generalization of the Decoupling Theorem to the case when the average is taken over an  $\varepsilon$ -almost 2-design instead of the whole unitary group, opening applications of this theorem in various physical situations. Chapters five, six and seven analyze the decoupling behavior of permutations. Potential applications lie in the areas of quantum cryptography and coding theory. The results of the chapters five and six are related to the General Leftover Hash Lemma, which is of significance for quantum cryptography [15]. Chapter seven aims at providing theorems for classical coding theory.

## 1.2 Notation and a glance at quantum mechanics

Throughout this thesis we will abide by the notational rules introduced in this section. One of the core objects of the mathematical description of some physical system  $A$  according to quantum mechanics is a complex Hilbert space  $\mathcal{H}_A$ , which we always will assume to have finite dimension,  $d_A$ . The space of linear operators on a Hilbert space  $\mathcal{H}$  will be denoted by  $\mathcal{L}(\mathcal{H})$ , the subspace of hermitian operators by  $\mathcal{L}^\dagger(\mathcal{H})$  and the set of positive-semidefinite operators is given by  $\mathcal{P}(\mathcal{H})$ . The set of normalized positive operators is given by  $\mathcal{S}_=(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) \mid \text{tr}\rho = 1\}$  and the set of subnormalized positive operators is  $\mathcal{S}_\leq(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) \mid \text{tr}\rho \leq 1\}$ . For those sets one has the following trivial inclusions:  $\mathcal{S}_=(\mathcal{H}) \subset \mathcal{S}_\leq(\mathcal{H}) \subset \mathcal{P}(\mathcal{H}) \subset \mathcal{L}^\dagger(\mathcal{H}) \subset \mathcal{L}(\mathcal{H})$ . More generally the vector space of homomorphisms of some Hilbert space  $\mathcal{H}_A$  to  $\mathcal{H}_B$  will be denoted by  $\text{Hom}(\mathcal{H}_A, \mathcal{H}_B)$ . For  $\varphi \in \mathcal{H}$ , the corresponding elements of the spaces  $\text{Hom}(\mathbb{C}, \mathcal{H})$  and  $\text{Hom}(\mathcal{H}, \mathbb{C})$  are denoted by  $|\varphi\rangle$  and  $\langle\varphi|$  respectively. Thus for example  $|\varphi\rangle\langle\varphi| \in \mathcal{P}(\mathcal{H})$  is a projector. Since the spaces  $\mathcal{H}_A$  and  $\text{Hom}(\mathbb{C}, \mathcal{H})$  are isomorphic, we sometimes will treat  $|\varphi\rangle$  as if it was an element of  $\mathcal{H}_A$ . In this cases we implicitly mean the unique corresponding element in  $\mathcal{H}_A$ .

If the quantum state of the system  $A$  is known with certainty, according to quantum mechanics it is represented by an element

$$[\varphi_A] := \{e^{i\alpha}\varphi_A \mid \varphi_A \in \mathcal{H}_A; \|\varphi_A\| = 1; \alpha \in [0, 2\pi]\}$$

of the projective Hilbert space belonging to  $\mathcal{H}_A$ , where an index letter following some mathematical object denotes to which physical system it belongs. More generally the quantum states of the system  $A$  are in one to one correspondence with the elements  $\rho_A$  of  $\mathcal{S}_=(\mathcal{H}_A)$ , even if the state of the system is not fully known to its observer. Since in quantum information theory usually only partial knowledge about some system  $A$  is given, the core object of study will be the density operator  $\rho_A$ , and we call  $\rho_A$  just the state of the system. Sometimes one considers joint systems  $AB$ , which, due to the postulates of quantum mechanics, are represented by a tensor product space  $\mathcal{H}_A \otimes \mathcal{H}_B =: \mathcal{H}_{AB}$ . Then the corresponding density operator will have a double index, too:  $\rho_{AB}$ . However, when it is clear which systems are represented by the density operators we might drop the indices to simplify the notation. We will denote with  $\mathbb{1}_A$  the identity operator on  $\mathcal{H}_A$  and with  $\pi_A := \frac{\mathbb{1}_A}{d_A}$  the completely mixed state on  $A$ . Moreover  $\Phi_{AB}$  is the completely entangled state on  $AB$  i.e.  $\Phi_{AB} := |\Phi\rangle\langle\Phi|_{AB}$ , where  $|\Phi\rangle_{AB} := \frac{1}{\sqrt{d_A}} \sum_i |i\rangle_A \otimes |i\rangle_B$  and  $d_A = d_B$  and the  $|i\rangle_A, |i\rangle_B$  form an orthonormal basis for  $\mathcal{H}_A$  and for  $\mathcal{H}_B$ , which is isomorphic to  $\mathcal{H}_A$ .



Linear maps from  $\mathcal{L}(\mathcal{H}_A)$  to  $\mathcal{L}(\mathcal{H}_B)$  will be denoted by the calligraphic letters  $\mathcal{T}_{A \rightarrow B}$ ,  $\mathcal{E}_{A \rightarrow B}$ ,  $\mathcal{N}_{A \rightarrow B}, \dots$ . Quantum operations are in one to one correspondence to the trace preserving and completely positive maps (TPCPM)  $\mathcal{T}_{A \rightarrow B}$  which map density operators to density operators. We sometimes will call a TPCP map also a *quantum channel*, if we want to emphasize the use of the TPCPM under consideration for information processing. The TPCPM we will encounter most often is the partial trace (over the system  $B$ ), which is given by a map  $\mathcal{E}_{AB \rightarrow A}$ , defined to be the adjoint mapping  $\mathcal{T}^\dagger$  of  $\mathcal{T}(\xi_A) = \xi_A \otimes \mathbb{1}_B$ ;  $\xi \in \mathcal{L}^\dagger(\mathcal{H})$  with respect to the Schmidt scalar product  $\langle A, B \rangle := \text{tr}(A^\dagger B)$ . That means  $\text{tr}(\mathcal{T}(\xi)\zeta) = \text{tr}(\xi\mathcal{T}^\dagger(\zeta))$ . It is used to determine the expectation values for measurements on a subsystem  $A$  if the state of some bipartite system  $AB$  is given. Because of its crucial importance the partial trace has a special notation:

$$\mathcal{E}_{AB \rightarrow A}(\zeta_{AB}) =: \text{tr}_B(\zeta_{AB}),$$

where  $\zeta_{AB}$  is any operator in  $\mathcal{L}^\dagger(\mathcal{H}_{AB})$ . If we have a bipartite state  $\xi_{AB}$  and we would like to consider a subsystem only, we will denote by  $\xi_A$  the partial trace of  $\xi_{AB}$  over the system  $B$ ,  $\xi_A = \text{tr}_B \xi_{AB}$ .

We will call  $\omega_{A'E} := (\mathcal{T}_{A \rightarrow E} \otimes \mathcal{I}_{A'}) (\Phi_{AA'})$  for any  $\mathcal{T}_{A \rightarrow E} \in \text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$  the Choi-Jamiolkowski representation [2, 11] of  $\mathcal{T}_{A \rightarrow E}$ , where  $\mathcal{H}_{A'}$  is a copy of  $\mathcal{H}_A$  and  $\mathcal{I}_{A'} \in \text{Hom}(\mathcal{L}(\mathcal{H}_{A'}), \mathcal{L}(\mathcal{H}_{A'}))$  denotes the operator identity. (Note that writing  $\omega_{A'E}$  we slightly abuse notation, since, strictly speaking,  $\omega_{A'E}$  is by definition an operator in  $\mathcal{L}(\mathcal{H}_E \otimes \mathcal{H}_{A'})$  and not in  $\mathcal{L}(\mathcal{H}_{A'} \otimes \mathcal{H}_E)$  as the notation indicates. This will be the only exception.) To keep the notation as simple as possible we have the convention that if a map  $\mathcal{T}_{A \rightarrow E}$  acts on a bipartite state with subsystem  $A$ , we mean that implicitly the identity is applied on the other subsystem. Thus we for example write  $\mathcal{T}_{A \rightarrow E}(\Phi_{AA'}) := (\mathcal{T}_{A \rightarrow E} \otimes \mathcal{I}_{A'}) (\Phi_{AA'})$  for the Choi-Jamiolkowski representation.

Any TPCPM can be viewed as a unitary operation on some larger system. More precisely speaking we have the following lemma [16]:

**Lemma 1:** (Stinespring dilation) *Let  $\mathcal{T}$  be a TPCPM from  $\mathcal{L}(\mathcal{H}_A)$  to  $\mathcal{L}(\mathcal{H}_B)$ . Then there exists some isometry  $U \in \text{Hom}(\mathcal{H}_A, \mathcal{H}_B \otimes \mathcal{H}_R)$  for some Hilbert space  $\mathcal{H}_R$ , such that*

$$\mathcal{T} : \rho_A \mapsto \text{tr}_R(U \rho_A U^\dagger).$$

Thus,  $\mathcal{T}$  can be viewed as a concatenation of two TPCP maps: First conjugating

$\rho_A$  with  $U$  and afterwards taking the partial trace over the system  $R$ . We will write shortly  $\mathcal{T} = \text{tr}_R \circ U \cdot$  for this operation.

To quantify whether a quantum state is preserved by some quantum operation (or more generally by some mapping  $\mathcal{T}$ ) or not, we have to introduce distance measures on the set of density operators. For any operator in  $\xi \in \mathcal{L}(\mathcal{H})$  we denote by  $\|\xi\|_1$  the Schatten 1-norm, by  $\|\xi\|_2$  the Schatten 2-norm, by  $\|\xi\|_F$  the Frobenius-norm and by  $\|\xi\|_\infty$  the  $\infty$ -norm of  $\xi$  which are defined to be

$$\|\xi\|_1 := \text{tr}|\xi| := \text{tr}(\sqrt{\xi^\dagger \xi}) \quad (1.1)$$

$$\|\xi\|_2 := \sqrt{\text{tr}(\xi^\dagger \xi)} \quad (1.2)$$

$$\|\xi\|_F := \sqrt{\sum_{i,j} |\xi_{ij}|^2} \quad (1.3)$$

$$\|\xi\|_\infty := \sqrt{\lambda_{\max}(\xi^\dagger \xi)} \quad (1.4)$$

respectively. Particularly that means that if  $\xi$  is in  $\mathcal{L}^\dagger(\mathcal{H})$ ,  $\|\xi\|_1$  is just equal to the sum of the absolute values of the eigenvalues of  $\xi$ . For our purposes it is sufficient to think of the Schatten 2-norm as the induced norm by the Schmidt scalar product. In contrast to the other norms above, the Frobenius-norm is an “entrywise” norm:  $\xi_{ij}$  are the entries of the matrix corresponding to the operator  $\xi$  in some basis. (We work in finite dimensions only.) It is a priori not clear that the norm defined in the above way is well defined but a short calculation reveals that  $\|\xi\|_F = \|\xi\|_2$  which also proofs that it actually can be seen as an operator norm ([1]). Finally the  $\infty$ -norm is given by the square root of the biggest eigenvalue  $\lambda_{\max}$  of  $\xi^\dagger \xi$  for any  $\xi \in \mathcal{L}(\mathcal{H})$ . We will frequently have to link the above norms in terms of inequalities. This is achieved using the following standard result ([22], *Lecture 3*):

**Lemma 2:** (Norm Inequalities) *For any  $A, B, C \in \mathcal{L}(\mathcal{H})$ , the following inequalities hold*

$$\|ABC\|_\infty \leq \|A\|_\infty \|B\|_\infty \|C\|_\infty,$$

$$\|ABC\|_1 \leq \|A\|_\infty \|B\|_1 \|C\|_\infty,$$

$$\|ABC\|_2 \leq \|A\|_\infty \|B\|_2 \|C\|_\infty.$$

The Schatten 1-norm induces a metric on  $\mathcal{S}_\leq(\mathcal{H})$ , which we call the *trace distance* and is defined (in this thesis) to be:

$$D(\rho, \sigma) := \|\rho - \sigma\|_1$$

In the special case that  $\rho$  and  $\sigma$  are elements of  $\mathcal{S}_=(\mathcal{H})$ , this gives a good distance measure in the sense that any measurement performed on states that are close in trace distance gives rise to probability distributions  $p, q$  that are close in the sense that the maximum difference of the probabilities that some event  $S$  occurs with respect to the different probability distributions  $\max_S(\sum_{x \in S} p_x - \sum_{x \in S} q_x)$  is small, too [14]. That means that those density operators cannot be well distinguished by any measurement. For positive operators with trace not equal to one this distance is not convenient. One therefore introduces a *generalized trace distance*,  $\bar{D}(\rho, \sigma)$ , which gives a good distance measure for sub-normalized states [20]:

$$\bar{D}(\rho, \sigma) := \|\rho - \sigma\|_1 + |\text{tr}\rho - \text{tr}\sigma|,$$

for any  $\rho, \sigma \in \mathcal{P}(\mathcal{H})$ . In the case of normalized states it reduces to the usual trace distance defined above.

Another commonly used measure of distance is the *fidelity*:

$$F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1,$$

for any density operators  $\rho, \sigma$ . The fidelity is not a metric on the states of some quantum system, but there are several types of metrics derived from it. In this thesis we will deal with the following one:

$$P(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}$$

Again this type of distance measure is not convenient for quantum information theory if the density operators are not normalized. In [20] the *purified distance*  $\bar{P}(\rho, \sigma)$  is introduced, which generalizes  $P(\rho, \sigma)$ :

$$\bar{P}(\rho, \sigma) := \sqrt{1 - \bar{F}(\rho, \sigma)^2},$$

where  $\bar{F}(\rho, \sigma)$  is the *generalized fidelity*:

$$\bar{F}(\rho, \sigma) := F(\rho, \sigma) + \sqrt{(1 - \text{tr}\rho)(1 - \text{tr}\sigma)},$$

for  $\rho, \sigma$  in  $\mathcal{S}_\leq(\mathcal{H})$ . Note that, if  $\rho$  or  $\sigma$  is in  $\mathcal{S}_=(\mathcal{H})$ , the generalized fidelity reduces to the usual one.

Both distance measures  $D(\rho, \sigma)$  and  $P(\rho, \sigma)$  introduced above are essentially equivalent, due to the following fundamental *Fuchs- van der Graaf inequalities* [14].

**Lemma 3:** (Fuchs- van der Graaf inequalities) *Let  $\rho, \sigma$  be in  $\mathcal{S}_=(\mathcal{H})$ , then*

$$\frac{1}{2}\|\rho - \sigma\|_1 \leq P(\rho, \sigma) \leq \sqrt{\|\rho - \sigma\|_1}.$$

Using the generalized versions of trace distance and the fidelity the authors derive in [20] the analogous relations for the generalized quantities:

**Lemma 4:** (Generalized Fuchs- van der Graaf inequalities) *Let  $\rho, \sigma$  be in  $\mathcal{S}_{\leq}(\mathcal{H})$ , then*

$$\frac{1}{2}\bar{D}(\rho, \sigma) \leq \bar{P}(\rho, \sigma) \leq \sqrt{\bar{D}(\rho, \sigma)}.$$

To quantify the uncertainty of our knowledge about some quantum state we use entropy measures. Various such measures are treated in the literature, for us the most important will be the quantum two-entropy and the min-entropy:

**Definition 1.** Let  $\rho_A$  be in  $\mathcal{P}(\mathcal{H}_A)$ . Then its min-entropy is defined to be

$$H_{\min}(A)_\rho := -\log \min\{\lambda \in \mathbb{R} \mid \rho_A \leq \lambda \mathbb{1}_A\}.$$

This is just the negative logarithm of the largest eigenvalue of  $\rho_A$ . We also require a conditional version of the min-entropy. Given a bipartite quantum system, conditional entropies in general aim to quantify the uncertainty, which we have about one of the subsystems if the state of the other subsystem is known.

**Definition 2.** Let  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ , then the min-entropy of  $A$  conditioned on  $B$  of  $\rho_{AB}$  is defined as [15, 20]

$$H_{\min}(A|B)_\rho := \max_{\sigma_B \in \mathcal{S}_{=}(\mathcal{H}_B)} \sup\{\lambda \in \mathbb{R} \mid \rho_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B\}.$$

Finally, we define the quantum conditional 2-entropy, which will occur in the statement of the decoupling theorem, but is only an auxiliary quantity from the point of view of information theory:

**Definition 3.** Let  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ , then the 2-entropy of  $A$  conditioned on  $B$  of  $\rho_{AB}$  is defined as

$$H_2(A|B)_\rho := -\log \min_{\sigma_B \in \mathcal{S}_{=}(\mathcal{H}_B)} \frac{1}{\text{tr}(\rho_{AB})} \text{tr}\left(\left((\mathbb{1}_A \otimes \sigma_B)^{-1/2} \rho_{AB}\right)^2\right)$$

The minimum is attained for a  $\sigma_B$  with  $\text{supp}\{\sigma_B\} \supset \text{supp}\{\rho_B\}$ , where  $\text{supp}\{\cdot\}$  denotes the support of some operator. Between the conditional min-entropy and the conditional two-entropy we have the following important relation, which links the auxiliary quantity  $H_2$  to the physical quantity  $H_{\min}$ :

**Lemma 5:** *Let  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ , then*

$$H_{\min}(A|B)_\rho \leq H_2(A|B)_\rho$$

This is just remark (5.3.2) in [15]. The proof of the statement can be found, there.

### 1.3 Induced neighborhoods and the smoothed conditional min-entropy

One can define a smoothed version of  $H_{\min}$  in the following way: Instead of evaluating  $H_{\min}$  at  $\rho$  directly one maximizes the min-entropy over a set of states that are  $\varepsilon$ -close to  $\rho$ . Obviously the crucial question is which distance measure should be used to determine  $\varepsilon$ -closeness? In [20] the authors show that the following type of  $\varepsilon$ -neighborhoods is particularly useful:

**Definition 4** ([20]). Let  $\varepsilon \geq 0$  and  $\rho \in \mathcal{S}_{\leq}(\mathcal{H})$  with  $\sqrt{\text{tr}\rho} > \varepsilon$ , then

$$\mathcal{B}^{\varepsilon}(\mathcal{H}; \rho) := \{\sigma \in \mathcal{S}_{\leq}(\mathcal{H}) \mid \bar{P}(\sigma, \rho) \leq \varepsilon\}.$$

This  $\varepsilon$ -ball can be used to define a smoothed version of the min-entropy:

**Definition 5** ([15, 20]). Let  $\varepsilon \geq 0$  and  $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ , then the  $\varepsilon$ -smooth min-entropy of  $A$  conditioned on  $B$  of  $\rho_{AB}$  is defined as

$$H_{\min}^{\varepsilon}(A|B)_{\rho} = \max_{\tilde{\rho} \in \mathcal{B}^{\varepsilon}(\rho)} H_{\min}(A|B)_{\tilde{\rho}}.$$

Many important properties of this entropy, including the proof of the fact that it actually is a continuous function of  $\rho$ , can be found in [20].

## Chapter 2

# Decoupling via the Schatten 2-norm

One of the main results of this thesis is a generalization of the decoupling theorem of [5] and [19] to the case when unitary almost 2-designs are considered only. The proof of this formula will be a generalized proof of the decoupling theorem, with major parts resembling the original proof in [5]. In this chapter we present a shorter proof of the original decoupling theorem with integration over the unitary group  $\mathbb{U}(A)$ . The methodology developed here will be relevant when proving the theorem's generalization in the next chapter. First we prove a lemma which provides an easy way of performing the required integration. This lemma will rely on a consideration of the Schatten 2-norm instead of the Schatten 1-norm and on working with the state  $\xi_{A\bar{A}} := \Phi_{A\bar{A}} - \pi_A \otimes \pi_{\bar{A}}$ . As a result we will obtain a slightly better bound than is given by the original decoupling theorem.

### 2.1 Lemma: Decoupling with the Schatten 2-norm

Many of the difficulties one has to overcome during the derivation of the decoupling theorem as in [5] arise from the fact that untill now we cannot integrate the square-root function. The idea therefore is to consider an integrand which does not contain any roots, instead. For this reason we will work with the Schatten 2-norm. In return the derived statement will be an equality, such that the converse of the theorem is valid automatically.

**Lemma:** (Decoupling Lemma) *Let  $\rho_{AR} \in \mathcal{L}^1(\mathcal{H}_A \otimes \mathcal{H}_R)$  and let  $\mathcal{T}_{A \rightarrow E} \in \text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$  be a linear map with Choi-Jamiolkowski representation*

$\omega_{A'E} \in \mathcal{L}^\dagger(\mathcal{H}_E \otimes \mathcal{H}_{A'})$ , then

$$\begin{aligned} & \int_{\mathbb{U}(A)} \left\| \mathcal{T}(U_A \otimes \mathbb{1}_R \rho_{AR} U_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_2^2 dU \\ &= \frac{d_A^2}{d_A^2 - 1} \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_2^2 \left\| \omega_{A'E} - \pi_{A'} \otimes \omega_E \right\|_2^2 \end{aligned}$$

where the integration goes over all unitaries and with respect to the probability Haar measure  $dU$ .

For the proof it will be convenient to reformulate the argument of the integral in a more symmetric way. We introduce the map  $\mathcal{E}_{\tilde{A} \rightarrow R}$ , which we define to be the unique Choi-Jamiolkowski preimage of the state  $\rho_{AR}$  i.e.  $\mathcal{E}_{\tilde{A} \rightarrow R}(\Phi_{A\tilde{A}}) = \rho_{AR}$ , where  $\tilde{A}$  is just a copy of  $A$ . Note that  $\mathcal{E}$  is not trace-preserving in general. Because  $\mathcal{E}$  acts only on the  $\tilde{A}$  subsystem and the identity is applied to the  $A$  part, taking the partial trace over  $A$  commutes with applying the map  $\mathcal{E}$  to  $\Phi_{A\tilde{A}}$ . We thus have

$$\rho_R = \text{tr}_A(\mathcal{E}(\Phi_{A\tilde{A}})) \quad (2.1)$$

$$= \mathcal{E}(\pi_{\tilde{A}}). \quad (2.2)$$

An analogous relation is also valid for  $\mathcal{T}_{A \rightarrow E}$  and we can write for any unitary  $U_A$ :

$$\begin{aligned} & \mathcal{T}((U_A \otimes \mathbb{1}_R) \rho_{AR} (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \\ &= \mathcal{T}((U_A \otimes \mathbb{1}_R) \mathcal{E}(\Phi_{A\tilde{A}}) (U_A^\dagger \otimes \mathbb{1}_R)) - \mathcal{T}(\pi_A) \otimes \mathcal{E}(\pi_{\tilde{A}}) \end{aligned} \quad (2.3)$$

$$= (\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}}) \Phi_{A\tilde{A}} (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})) - (\mathcal{T} \otimes \mathcal{E})(\pi_A \otimes \pi_{\tilde{A}}) \quad (2.4)$$

$$= (\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}}) (\Phi_{A\tilde{A}} - \pi_A \otimes \pi_{\tilde{A}}) (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})) \quad (2.5)$$

$$= (\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}}) (\xi_{A\tilde{A}}) (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})) \quad (2.6)$$

In equation (2.4), we used the fact that the unitary applied only acts on the  $A$  subsystem in contrast to  $\mathcal{E}$  which acts on  $R$  only and therefore the operations of conjugation with  $U_A$  and applying  $\mathcal{E}$  commute. In the last equation (2.6) we introduce the *decoupling state*  $\xi_{A\tilde{A}} := \Phi_{A\tilde{A}} - \pi_A \otimes \pi_{\tilde{A}}$  for notational convenience. We will later see an interesting property of this state.

This way of writing the integrand of the usual decoupling theorem yields a shorter proof of the theorem, since the mixed terms in [5] do not have to be considered anymore. Moreover the proof gets “symmetric” in the treatment of  $\rho_{AR}$  and  $\omega_{A'E}$  which will be of crucial relevance, at the moment when we will have to apply the

definition of the almost 2-design and find upper bounds in the case of the generalized theorem. Note that by (2.2) we have in addition that

$$\mathcal{E}(\xi_{A\bar{A}}) = \rho_{AR} - \pi_A \otimes \rho_R \wedge \mathcal{T}(\xi_{A\bar{A}}) = \omega_{\bar{A}E} - \pi_{\bar{A}} \otimes \omega_E. \quad (2.7)$$

Thus the stated lemma can be rewritten equivalently in terms of the decoupling state. We note that

$$\frac{d_A^2}{d_A^2 - 1} = \frac{1}{\|\xi_{A\bar{A}}\|_2^2} \quad (2.8)$$

and obtain:

**Lemma:** (Decoupling Lemma) *Let  $\xi_{A\bar{A}} = \Phi_{A\bar{A}} - \pi_{\bar{A}} \otimes \pi_{\bar{A}}$  and let  $\mathcal{T}_{A \rightarrow E} \in \text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$  and  $\mathcal{E}_{\bar{A} \rightarrow R} \in \text{Hom}(\mathcal{L}(\mathcal{H}_{\bar{A}}), \mathcal{L}(\mathcal{H}_R))$  be linear maps then*

$$\int_{\mathbb{U}(A)} \|(\mathcal{T} \otimes \mathcal{E})(U_A \otimes \mathbb{1}_{\bar{A}} \xi_{A\bar{A}} U_A^\dagger \otimes \mathbb{1}_{\bar{A}})\|_2^2 dU = \frac{\|\mathcal{E}(\xi_{A\bar{A}})\|_2^2 \|\mathcal{T}(\xi_{A\bar{A}})\|_2^2}{\|\xi_{A\bar{A}}\|_2^2}$$

where the integration goes over all unitaries and with respect to the probability Haar measure  $dU$ .

This formulation is especially convenient for the proof. We have that

$$\begin{aligned} & \int_{\mathbb{U}(A)} \|(\mathcal{T} \otimes \mathcal{E})(U_A \otimes \mathbb{1}_{\bar{A}} \xi_{A\bar{A}} U_A^\dagger \otimes \mathbb{1}_{\bar{A}})\|_2^2 dU \\ &= \int_{\mathbb{U}(A)} \text{tr}((\mathcal{T} \otimes \mathcal{E})(U_A \otimes \mathbb{1}_{\bar{A}} \xi_{A\bar{A}} U_A^\dagger \otimes \mathbb{1}_{\bar{A}})^2) dU \end{aligned} \quad (2.9)$$

$$= \int_{\mathbb{U}(A)} \text{tr}((\mathcal{T} \otimes \mathcal{E})^{\otimes 2}((U_A \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} (\xi_{A\bar{A}})^{\otimes 2} (U_A^\dagger \otimes \mathbb{1}_{\bar{A}})^{\otimes 2}) \mathcal{F}_{ER}) dU \quad (2.10)$$

$$= \int_{\mathbb{U}(A)} \text{tr}(((U_A \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} (\xi_{A\bar{A}})^{\otimes 2} (U_A^\dagger \otimes \mathbb{1}_{\bar{A}})^{\otimes 2}) (\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\mathcal{E}^\dagger)^{\otimes 2}[\mathcal{F}_R]) dU. \quad (2.11)$$

We introduced two further copies  $A'$  and  $\tilde{A}'$  of  $A$  when using the swap trick (see Appendix C) in equation (2.10), i.e.  $(\xi_{A\bar{A}})^{\otimes 2} = \xi_{A\bar{A}} \otimes \xi_{A'\bar{A}'}$ . In equation (2.11) we used the definition of the adjoint of the mapping  $(\tilde{\mathcal{T}} \otimes \tilde{\mathcal{E}})^{\otimes 2}$  with respect to the Schmidt scalar product. Note that this map has product structure and since we apply it on a product state the two different parts  $(\tilde{\mathcal{T}})^{\otimes 2}$  and  $(\tilde{\mathcal{E}})^{\otimes 2}$  can be applied separately. At this point it is not difficult to perform the integration on  $(\xi_{A\bar{A}})^{\otimes 2}$  directly but it is known from [5, 10] that

$$\int [(U_A)^\dagger]^{\otimes 2} (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} (\mathcal{F}_E) (U_A)^{\otimes 2} dU = \alpha \mathbb{1}_{AA'} + \beta \mathcal{F}_A, \quad (2.12)$$



with the coefficients  $\alpha$  and  $\beta$  satisfying

$$\alpha = \text{tr}(\omega_{\text{E}}^2) \left( \frac{d_{\text{A}}^2 - \frac{d_{\text{A}} \text{tr}(\omega_{\text{A}'\text{E}}^2)}{\text{tr}(\omega_{\text{E}}^2)}}{d_{\text{A}}^2 - 1} \right) \quad (2.13)$$

$$\beta = \text{tr}(\omega_{\text{A}'\text{E}}^2) \left( \frac{d_{\text{A}}^2 - \frac{d_{\text{A}} \text{tr}(\omega_{\text{E}}^2)}{\text{tr}(\omega_{\text{A}'\text{E}}^2)}}{d_{\text{A}}^2 - 1} \right). \quad (2.14)$$

Thus it is even less work to perform the integration over  $(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}(\mathcal{F}_{\text{E}})$ . We get that

$$\begin{aligned} & \int_{\mathbb{U}(A)} \left\| (\mathcal{T} \otimes \mathcal{E})(U_{\text{A}} \otimes \mathbb{1}_{\tilde{\text{A}}} \xi_{\text{A}\tilde{\text{A}}} U_{\text{A}}^\dagger \otimes \mathbb{1}_{\tilde{\text{A}}}) \right\|_2^2 dU \\ &= \int_{\mathbb{U}(A)} \text{tr} \left( (\xi_{\text{A}\tilde{\text{A}}})^{\otimes 2} (U_{\text{A}}^\dagger)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{E}}] (U_{\text{A}})^{\otimes 2} \otimes (\mathcal{E}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{R}}] \right) dU \end{aligned} \quad (2.15)$$

$$= \text{tr} \left( (\xi_{\text{A}\tilde{\text{A}}})^{\otimes 2} \{ \alpha \mathbb{1}_{\text{A}\text{A}'} + \beta \mathcal{F}_{\text{A}} \} \otimes (\mathcal{E}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{R}}] \right) \quad (2.16)$$

$$= \alpha \text{tr} \left( (\xi_{\text{A}\tilde{\text{A}}})^{\otimes 2} \mathbb{1}_{\text{A}\text{A}'} \otimes (\mathcal{E}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{R}}] \right) + \beta \text{tr} \left( (\xi_{\text{A}\tilde{\text{A}}})^{\otimes 2} \mathcal{F}_{\text{A}} \otimes (\mathcal{E}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{R}}] \right) \quad (2.17)$$

$$= \beta \text{tr} \left( (\xi_{\text{A}\tilde{\text{A}}})^{\otimes 2} \mathcal{F}_{\text{A}} \otimes (\mathcal{E}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{R}}] \right). \quad (2.18)$$

In the last step we used that tracing out one of the subsystems  $A, \tilde{A}$  of  $(\xi_{\text{A}\tilde{\text{A}}})$  gives the zero state. Using the definition of the adjoint of  $\mathcal{E}$  we find

$$\beta \text{tr} \left( (\xi_{\text{A}\tilde{\text{A}}})^{\otimes 2} \mathcal{F}_{\text{A}} \otimes (\mathcal{E}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{R}}] \right) = \beta \text{tr} \left( \mathcal{E}(\xi_{\text{A}\tilde{\text{A}}})^{\otimes 2} \mathcal{F}_{\text{AR}} \right) \quad (2.19)$$

$$= \beta \text{tr} \left( \mathcal{E}(\xi_{\text{A}\tilde{\text{A}}})^2 \right) \quad (2.20)$$

$$= \beta \left\| \mathcal{E}(\xi_{\text{A}\tilde{\text{A}}}) \right\|_2^2. \quad (2.21)$$

Rewriting  $\beta$  we find that

$$\beta = \text{tr}(\omega_{A'E}^2) \left( \frac{d_A^2 - \frac{d_A \text{tr}(\omega_E^2)}{\text{tr}(\omega_{A'E}^2)}}{d_A^2 - 1} \right) \quad (2.22)$$

$$= \frac{d_A^2}{d_A^2 - 1} \left( \text{tr}(\omega_{A'E}^2) - \frac{1}{d_A} \text{tr}(\omega_E^2) \right) \quad (2.23)$$

$$= \frac{d_A^2}{d_A^2 - 1} \left( \text{tr}(\omega_{A'E}^2) - 2\frac{1}{d_A} \text{tr}(\omega_E^2) + \frac{1}{d_A} \text{tr}(\omega_E^2) \right) \quad (2.24)$$

$$= \frac{d_A^2}{d_A^2 - 1} \left( \text{tr}(\omega_{A'E}^2) - 2\frac{1}{d_A} \text{tr}(\mathbb{1}_{A'} \otimes \omega_E \omega_{A'E}) + \text{tr}(\pi_A^2 \otimes \omega_E^2) \right) \quad (2.25)$$

$$= \frac{d_A^2}{d_A^2 - 1} \text{tr}((\omega_{A'E} - \pi_{A'} \otimes \omega_E)^2) \quad (2.26)$$

$$= \frac{d_A^2}{d_A^2 - 1} \text{tr}(\mathcal{T}(\xi_{A\bar{A}})^2) \quad (2.27)$$

$$= \frac{d_A^2}{d_A^2 - 1} \|\mathcal{T}(\xi_{A\bar{A}})\|_2^2. \quad (2.28)$$

We conclude plugging this into equation (2.21) that

$$\begin{aligned} & \int_{\mathbb{U}(A)} \left\| (\mathcal{T} \otimes \mathcal{E})(U_A \otimes \mathbb{1}_{\bar{A}} \xi_{A\bar{A}} U_A^\dagger \otimes \mathbb{1}_{\bar{A}}) \right\|_2^2 dU \\ &= \frac{d_A^2}{d_A^2 - 1} \|\mathcal{T}(\xi_{A\bar{A}})\|_2^2 \|\mathcal{E}(\xi_{A\bar{A}})\|_2^2, \end{aligned} \quad (2.29)$$

which proofs the decoupling lemma.

## 2.2 An alternative proof of the decoupling theorem

As an application of the last section's lemma, we shortly rederive the decoupling theorem of [5] in the formulation which is given in [19].

**Theorem:** (Decoupling theorem) *Let  $\rho_{AR} \in \mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_R)$  be a sub normalized density operator and let  $\mathcal{T}_{A \rightarrow E}$  be a completely positive linear map going from  $\mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_R)$  to  $\mathcal{P}(\mathcal{H}_E \otimes \mathcal{H}_R)$  with Choi-Jamiolkowski representation  $\omega_{A'E} \in \mathcal{S}_{\leq}(\mathcal{H}_E \otimes \mathcal{H}_{A'})$ , then*

$$\int_{\mathbb{U}(A)} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R) \rho_{AR} (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\|_1 dU \leq 2^{-\frac{1}{2}H_2(A'|E)_\omega - \frac{1}{2}H_2(A|R)_\rho}$$

where the integration goes over all unitaries and with respect to the probability Haar measure  $dU$ .

The proof goes as follows. As we did in (2.6), we work with the integrand in terms of the decoupling state. We then use the Hölder inequality as stated in Appendix A with parameters  $r = t = 4$  and  $s = 2$  (or alternatively *Lemma 4* in [19]) to bound the Schatten 1-norm of the integrand in terms of the Schatten 2-norm:

$$\|ABC\|_1 \leq \| |A|^4 \|_1^{\frac{1}{4}} \| |B|^2 \|_1^{\frac{1}{2}} \| |C|^4 \|_1^{\frac{1}{4}} \quad (2.30)$$

Note that the term  $\| |B|^2 \|_1^{\frac{1}{2}}$  is just the Schatten 2-norm of  $B$ . Introducing the positive definite and normalized operators  $\sigma_E$  and  $\zeta_R$  with

$$A := (\sigma_E \otimes \zeta_R)^{\frac{1}{4}}, \quad (2.31)$$

$$B := (\sigma_E \otimes \zeta_R)^{-\frac{1}{4}} ((\mathcal{T} \otimes \mathcal{E})(U_A \otimes \mathbb{1}_{\bar{A}} \xi_{A\bar{A}} U_A^\dagger \otimes \mathbb{1}_{\bar{A}})) (\sigma_E \otimes \zeta_R)^{-\frac{1}{4}}, \quad (2.32)$$

$$C := (\sigma_E \otimes \zeta_R)^{\frac{1}{4}}. \quad (2.33)$$

the above (2.30) specializes to

$$\begin{aligned} & \|(\mathcal{T} \otimes \mathcal{E})(U_A \otimes \mathbb{1}_{\bar{A}} \xi_{A\bar{A}} U_A^\dagger \otimes \mathbb{1}_{\bar{A}})\|_1 \\ & \leq \left\| (\sigma_E \otimes \zeta_R)^{-\frac{1}{4}} ((\mathcal{T} \otimes \mathcal{E})(U_A \otimes \mathbb{1}_{\bar{A}} \xi_{A\bar{A}} U_A^\dagger \otimes \mathbb{1}_{\bar{A}})) (\sigma_E \otimes \zeta_R)^{-\frac{1}{4}} \right\|_2. \end{aligned} \quad (2.34)$$

One can abbreviate the notation introducing the completely positive map  $\tilde{\mathcal{T}}_{A \rightarrow E}$  with  $\tilde{\mathcal{T}}(\tau_{A\bar{A}}) := (\sigma_E \otimes \mathbb{1}_{\bar{A}})^{-1/4} \mathcal{T}(\tau_{A\bar{A}}) (\sigma_E \otimes \mathbb{1}_{\bar{A}})^{-1/4}$  for any  $\tau_{A\bar{A}} \in \mathcal{L}(\mathcal{H}_{A\bar{A}})$  and similarly the map  $\tilde{\mathcal{E}}_{\bar{A} \rightarrow R}$  is defined to be  $\tilde{\mathcal{E}}(\tau_{A\bar{A}}) := (\mathbb{1}_A \otimes \zeta_R)^{-1/4} \mathcal{E}(\tau_{A\bar{A}}) (\mathbb{1}_A \otimes \zeta_R)^{-1/4}$  for any  $\tau_{A\bar{A}} \in \mathcal{L}(\mathcal{H}_{A\bar{A}})$ . With the short notation we have

$$\begin{aligned} & \int_{\mathbb{U}(A)} \|(\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\bar{A}})(\xi_{A\bar{A}})(U_A^\dagger \otimes \mathbb{1}_{\bar{A}}))\|_1^2 dU \\ & \leq \int_{\mathbb{U}(A)} \|(\tilde{\mathcal{T}} \otimes \tilde{\mathcal{E}})((U_A \otimes \mathbb{1}_{\bar{A}})(\xi_{A\bar{A}})(U_A^\dagger \otimes \mathbb{1}_{\bar{A}}))\|_2^2 dU \end{aligned} \quad (2.35)$$

$$= \frac{d_A^2}{d_A^2 - 1} \left\| \tilde{\mathcal{T}}(\xi_{A\bar{A}}) \right\|_2^2 \left\| \tilde{\mathcal{E}}(\xi_{A\bar{A}}) \right\|_2^2, \quad (2.36)$$

where we applied the *Decoupling Lemma* in the last step. Going the steps from (2.22) to (2.28) backwards gives:

$$\begin{aligned} & \frac{d_A^2}{d_A^2 - 1} \left\| \tilde{\mathcal{T}}(\xi_{A\tilde{A}}) \right\|_2^2 \left\| \tilde{\mathcal{E}}(\xi_{A\tilde{A}}) \right\|_2^2 \\ &= \left(1 - \frac{1}{d_A^2}\right) \text{tr}(\tilde{\omega}_{A'E}^2) \text{tr}(\tilde{\rho}_{AR}^2) \left( \frac{d_A^2 - \frac{d_A \text{tr}(\tilde{\omega}_E^2)}{\text{tr}(\tilde{\omega}_{A'E}^2)}}{d_A^2 - 1} \right) \left( \frac{d_A^2 - \frac{d_A \text{tr}(\tilde{\rho}_R^2)}{\text{tr}(\tilde{\rho}_{AR}^2)}}{d_A^2 - 1} \right) \end{aligned} \quad (2.37)$$

$$\leq \left(1 - \frac{1}{d_A^2}\right) \text{tr}(\tilde{\omega}_{A'E}^2) \text{tr}(\tilde{\rho}_{AR}^2) \quad (2.38)$$

$$\leq \text{tr}(\tilde{\omega}_{A'E}^2) \text{tr}(\tilde{\rho}_{AR}^2) \quad (2.39)$$

$$\leq \frac{1}{\text{tr}[\omega_{A'E}]} \text{tr} \left( ((\sigma_E^{-1/2} \otimes \mathbb{1}_{A'}) \omega_{A'E})^2 \right) \frac{1}{\text{tr}[\rho_{AR}]} \text{tr} \left( ((\mathbb{1}_A \otimes \zeta_R^{-1/2}) \rho_{AR})^2 \right) \quad (2.40)$$

In equation (2.38) we used *Lemma 3.5* in [5] (see also: [10]) to obtain that both bracket terms are smaller than one. The last inequality follows from the fact that both  $\omega_{A'E}$  and  $\rho_{AR}$  are sub normalized by the assumptions of the theorem. The whole derivation is valid for any positive and normalized operators  $\sigma_E$  and  $\zeta_R$ , therefore we can choose  $\sigma_E^*$  and  $\zeta_R^*$  such that they minimize the expression in (2.40). We get

$$\begin{aligned} & \int_{\mathbb{U}(A)} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R) \rho_{AR} (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\|_1^2 dU \\ & \leq \min_{\sigma_E \in \mathcal{S}=(\mathcal{H}_E)} \frac{1}{\text{tr}[\omega_{A'E}]} \text{tr} \left( ((\sigma_E^{-1/2} \otimes \mathbb{1}_{A'}) \omega_{A'E})^2 \right) \min_{\zeta_R \in \mathcal{S}=(\mathcal{H}_R)} \frac{1}{\text{tr}[\rho_{AR}]} \text{tr} \left( ((\mathbb{1}_A \otimes \zeta_R^{-1/2}) \rho_{AR})^2 \right) \end{aligned} \quad (2.41)$$

$$= 2^{-H_2(A|E)_\omega - H_2(A|R)_\rho}. \quad (2.42)$$

After taking the square root and applying the Jensen inequality (Appendix B), we recapture the decoupling theorem.

We note that in the above calculation we had to go back the steps from (2.22) to (2.28) and to use several bounds to obtain expressions with the “unphysical”  $H_2$ -entropy. It therefore seems that one should try to go to the  $H_{\min}$ -entropy directly. This is done in the following section.

## 2.3 An improved bound for the decoupling theorem

We reconsider formula (2.36) and write it out using the hidden operators  $\sigma_E$  and  $\zeta_R$ .

$$\begin{aligned} & \int_{\mathbb{U}(A)} \left\| (\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\bar{A}})(\xi_{A\bar{A}})(U_A^\dagger \otimes \mathbb{1}_{\bar{A}})) \right\|_1^2 dU \\ & \leq \frac{d_A^2}{d_A^2 - 1} \left\| \tilde{\mathcal{T}}(\xi_{A\bar{A}}) \right\|_2^2 \left\| \tilde{\mathcal{E}}(\xi_{A\bar{A}}) \right\|_2^2 \end{aligned} \quad (2.43)$$

$$\begin{aligned} & = \frac{d_A^2}{d_A^2 - 1} \left\| \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{4}} (\rho_{AR} - \pi_A \otimes \rho_R) \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{4}} \right\|_2^2 \\ & \quad \left\| \mathbb{1}_{A'} \otimes \sigma_E^{-\frac{1}{4}} (\omega_{A'E} - \pi_{A'} \otimes \omega_E) \mathbb{1}_{A'} \otimes \sigma_E^{-\frac{1}{4}} \right\|_2^2 \end{aligned} \quad (2.44)$$

Due to the similarity of the two terms with the Schatten 2-norm above it is sufficient to bound one of them. We choose the first and use the definition of the Schatten 2-norm to find

$$\left\| \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{4}} (\rho_{AR} - \pi_A \otimes \rho_R) \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{4}} \right\|_2^2 \quad (2.45)$$

$$\begin{aligned} & = \text{tr} \left( \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} (\rho_{AR} - \pi_A \otimes \rho_R) \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} (\rho_{AR} - \pi_A \otimes \rho_R) \right) \\ & \leq \left\| \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} (\rho_{AR} - \pi_A \otimes \rho_R) \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} (\rho_{AR} - \pi_A \otimes \rho_R) \right\|_1 \end{aligned} \quad (2.46)$$

$$\leq \left\| \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} (\rho_{AR} - \pi_A \otimes \rho_R) \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} \right\|_\infty \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_1. \quad (2.47)$$

The last inequality was obtained by an application of *Lemma 2*. Now we rewrite the expression with the  $\infty$ -norm in a way that reveals its relation to the  $H_{\min}$ -entropy. For this we choose from the beginning of our calculation on  $\zeta_R$  to minimize the term

with the  $\infty$ -norm i. e. we evaluate

$$\begin{aligned} & \min_{\zeta_R \in \mathcal{S}_=(H_R)} \left\| \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} (\rho_{AR} - \pi_A \otimes \rho_R) \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} \right\|_{\infty} \\ &= \min \left\{ \lambda \in \mathbb{R} \mid \lambda = \left\| \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} (\rho_{AR} - \pi_A \otimes \rho_R) \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} \right\|_{\infty}; \zeta_R \in \mathcal{S}_=(H_R) \right\} \end{aligned} \quad (2.48)$$

$$= \min \left\{ \lambda \in \mathbb{R} \mid \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} (\rho_{AR} - \pi_A \otimes \rho_R) \mathbb{1}_A \otimes \zeta_R^{-\frac{1}{2}} \leq \lambda \mathbb{1}_{AR}; \zeta_R \in \mathcal{S}_=(H_R) \right\} \quad (2.49)$$

$$= \min \{ \lambda \in \mathbb{R} \mid \rho_{AR} - \pi_A \otimes \rho_R \leq \lambda \mathbb{1}_A \otimes \zeta_R; \zeta_R \in \mathcal{S}_=(H_R) \} \quad (2.50)$$

$$= \min \left\{ \text{tr}(\zeta_R) \mid \rho_{AR} \leq \mathbb{1}_A \otimes (\zeta_R + \frac{1}{d_A} \rho_R); \zeta_R \in \mathcal{P}(H_R) \right\} \quad (2.51)$$

$$= \min \left\{ \text{tr} \left( \tilde{\zeta}_R - \frac{1}{d_A} \rho_R \right) \mid \rho_{AR} \leq \mathbb{1}_A \otimes \tilde{\zeta}_R; \tilde{\zeta}_R \in \mathcal{P}(H_R) + \frac{1}{d_A} \rho_R \right\} \quad (2.52)$$

$$= \min \left\{ \text{tr} \left( \zeta_R - \frac{1}{d_A} \rho_R \right) \mid \rho_{AR} \leq \mathbb{1}_A \otimes \zeta_R; \zeta_R \in \mathcal{P}(H_R) \right\} \quad (2.53)$$

$$= \min \{ \text{tr}(\zeta_R) \mid \rho_{AR} \leq \mathbb{1}_A \otimes \zeta_R; \zeta_R \in \mathcal{P}(H_R) \} - \frac{1}{d_A} \text{tr}(\rho_R) \quad (2.54)$$

$$= \min \{ \lambda \in \mathbb{R} \mid \rho_{AR} \leq \lambda \mathbb{1}_A \otimes \zeta_R; \zeta_R \in \mathcal{S}_=(H_R) \} - \frac{1}{d_A} \text{tr}(\rho_R) \quad (2.55)$$

$$= 2^{\min \{ \lambda \in \mathbb{R} \mid \rho_{AR} \leq 2^\lambda \mathbb{1}_A \otimes \zeta_R; \zeta_R \in \mathcal{S}_=(H_R) \}} - \frac{1}{d_A} \text{tr}(\rho_R) \quad (2.56)$$

$$= 2^{-H_{\min}(A|R)_\rho} - \frac{1}{d_A} \text{tr}(\rho_R). \quad (2.57)$$

For the last equality we used the definition of the  $H_{\min}$ -entropy. In equation (2.52) we exploited the fact that the sum of two positive-semidefinite matrices is given by a positive-semidefinite matrix again. Therefore the two groups (together with +)  $\mathcal{P}(H_R) + \frac{1}{d_A} \rho_R$  and  $\mathcal{P}(H_R)$  are identical. By analogy we can conclude that

$$\begin{aligned} & \left\| \mathbb{1}_{A'} \otimes \sigma_E^{-\frac{1}{4}} (\omega_{A'E} - \pi_{A'} \otimes \omega_E) \mathbb{1}_{A'} \otimes \sigma_E^{-\frac{1}{4}} \right\|_2^2 \\ & \leq \left( 2^{-H_{\min}(A'|E)_\omega} - \frac{1}{d_A} \text{tr}(\omega_E) \right) \left\| \omega_{A'E} - \pi_{A'} \otimes \omega_E \right\|_1. \end{aligned} \quad (2.58)$$

Plugging in both results into equation (2.44), we conclude

$$\begin{aligned} & \int_{\mathbb{U}(A)} \left\| (\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\bar{A}})(\xi_{A\bar{A}})(U_A^\dagger \otimes \mathbb{1}_{\bar{A}})) \right\|_1^2 dU \\ & \leq \frac{1}{1 - \frac{1}{d_A^2}} \left( 2^{-H_{\min}(A'|E)_\omega} - \frac{1}{d_A} \text{tr}(\omega_E) \right) \left( 2^{-H_{\min}(A|R)_\rho} - \frac{1}{d_A} \text{tr}(\rho_R) \right) \\ & \quad \left\| \omega_{A'E} - \pi_{A'} \otimes \omega_E \right\|_1 \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_1. \end{aligned} \quad (2.59)$$

Note that the  $H_{\min}$ -entropy is upper bounded by the logarithm of the dimension i. e.  $H_{\min}(A|R)_\rho \leq \log d_A$ , for example. Since the states  $\omega_{A'E}$  and  $\rho_{AR}$  are sub normalized by the conditions of the theorem, both bracket terms must be positive. This implies that the subtrahends in the brackets may be left out to obtain a shorter formulation of the result.

As a final step we perform the square root on both sides of (2.59) and then use Jensen inequality to be able to take the square root of the integrand. We find that

$$\begin{aligned} & \int_{\mathbb{U}(A)} \left\| (\mathcal{T} \otimes \mathcal{E})(U_A \otimes \mathbb{1}_{\tilde{A}})(\xi_{A\tilde{A}})(U_A^\dagger \otimes \mathbb{1}_{\tilde{A}}) \right\|_1 dU \\ & \leq \sqrt{\frac{1}{1 - \frac{1}{d_A^2}} \left( 2^{-H_{\min}(A'|E)_\omega} - \frac{1}{d_A} \text{tr}(\omega_E) \right) \left( 2^{-H_{\min}(A|R)_\rho} - \frac{1}{d_A} \text{tr}(\rho_R) \right)} \\ & \quad \sqrt{\left\| \omega_{A'E} - \pi_A \otimes \omega_E \right\|_1 \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_1} \end{aligned} \quad (2.60)$$

and arrive at a better bound for the decoupling theorem. We state our new version of the theorem for completeness:

**Theorem:** (Decoupling theorem) *Let  $\rho_{AR} \in \mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_R)$  be a sub normalized density operator and let  $\mathcal{T}_{A \rightarrow E}$  be a completely positive linear map going from  $\mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_R)$  to  $\mathcal{P}(\mathcal{H}_E \otimes \mathcal{H}_R)$  with Choi-Jamolkowski representation  $\omega_{A'E} \in \mathcal{S}_{\leq}(\mathcal{H}_E \otimes \mathcal{H}_{A'})$ , then*

$$\begin{aligned} & \int_{\mathbb{U}(A)} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R) \rho_{AR} (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\|_1 dU \\ & \leq \sqrt{\frac{1}{1 - \frac{1}{d_A^2}} \left( 2^{-H_{\min}(A'|E)_\omega} - \frac{1}{d_A} \text{tr}(\omega_E) \right) \left( 2^{-H_{\min}(A|R)_\rho} - \frac{1}{d_A} \text{tr}(\rho_R) \right)} \\ & \quad \sqrt{\left\| \omega_{A'E} - \pi_A \otimes \omega_E \right\|_1 \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_1} \end{aligned}$$

where the integration goes over all unitaries and with respect to the probability Haar measure  $dU$ .

In the sequel we will always work with the original decoupling theorem and we will not consider this version anymore. Thus when we refer to the ‘‘Decoupling Theorem’’, we always mean the original one as stated in the last section. All future results related to the original decoupling theorem can easily be generalized to formulations including the latest version. (This is for example the case for the main theorem about decoupling with almost 2-designs.)

## Chapter 3

# Decoupling with almost 2-designs

We consider the situation of a system  $A$  on which some physical process described by a unitary operation occurs. Generally we allow for correlations of the system  $A$  to a reference system  $R$ , on which no physical evolution takes place. Afterwards a TPCPM  $\mathcal{T}_{A \rightarrow E}$  is applied to the  $A$  subsystem again leaving the  $R$  subsystem unaffected. The joint state of the system  $AR$  before any process takes place is described by the density operator  $\rho_{AR}$ . Accordingly, the state of the system after the whole evolution is given by  $\mathcal{T}_{A \rightarrow E}(U_A \otimes \mathbb{1}_R \rho_{AR} U_A^\dagger \otimes \mathbb{1}_R)$ . For fixed  $\mathcal{T}$  and  $\rho_{AR}$  the Decoupling Theorem can be used to guarantee the existence of some unitary operator, such that applying that unitary and afterwards the map  $\mathcal{T}$  on the  $A$  subsystem of  $\rho_{AR}$  destroys almost all correlations between the two subsystems: Since we know that the average distance is bounded by

$$\int_{\mathbb{U}(A)} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R) \rho_{AR} (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\|_1 dU \leq 2^{-\frac{1}{2}H_2(A'|E)_\omega - \frac{1}{2}H_2(A|R)_\rho} \quad (3.1)$$

we can be sure that there exists a unitary  $U^*$  that decouples well in the sense that

$$\left\| \mathcal{T}((U_A^* \otimes \mathbb{1}_R) \rho_{AR} ((U_A^*)^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\|_1 \leq 2^{-\frac{1}{2}H_2(A'|E)_\omega - \frac{1}{2}H_2(A|R)_\rho}. \quad (3.2)$$

This is especially relevant for channel coding, since that unitary can be interpreted as an encoding operator [5, 8, 10]. In this chapter we go a step further and try to generalize the decoupling theorem to the case where we have an “almost-integration” only. As a motivation, we consider a concrete physical realization of the systems  $A$  and  $R$  assuming them to be made of interacting particles. We model the internal dynamics of the  $A$  subsystem in terms of a random quantum circuit and address the question whether or not a *physical* process occurring on the  $A$  subsystem may be used for encoding purposes. This means that some TPCPM  $\mathcal{T}_{A \rightarrow E}$  is fixed, and we analyze if a random quantum circuit does well in the sense of decoupling. This question is



particularly relevant for applications in case that  $\mathcal{T}$  is given by the partial trace. By the usual formulation of the decoupling theorem we already know that there exists some hypothetical physical process on the  $A$  subsystem which decouples well. But here we have a concrete model of the internal dynamics and we would like to see if these dynamics actually can produce the desired process. And how long would this take? We would like to give a precise meaning to this question using the concepts of *unitary designs* and *quantum circuits* in the following sections.

### 3.1 Unitary 2-designs

Suppose we are interested in taking the average of a function  $f$  over the Lie group  $\mathbb{U}$ . To obtain a guess about this value it is helpful to take a finite set  $\mathcal{D}$  of unitaries and instead evaluate  $f$  at these points and average over  $\mathcal{D}$ . This procedure is fairly similar to the the well known calculation of “upper sums” and “lower sums” in the definition of the Riemann integral over a subset of  $\mathbb{R}$ . (But here we don’t take the limit to infinite partitions). Of course for any such set there are functions  $f$  whose average over  $\mathbb{U}$  is arbitrarily different from the one over  $\mathcal{D}$ . But if we fix a certain type of “good” functions and assume the set  $\mathcal{D}$  to be “large” enough, we should obtain at least a good guess. Heuristically, a unitary  $k$ -designs is a finite subset  $\mathcal{D}$  of the Lie group  $\mathbb{U}$  that has the property that integrating any polynomial of degree  $k$  over the whole unitary group with respect to the Haar measure gives the same result as averaging over  $\mathcal{D}$ . We fix the vague statements from above in a definition [7]:

**Definition 6.** (Unitary design) Let  $\mathcal{D} = \{U_i\}_{i=1,\dots,n}$  be a set of unitary matrices on a Hilbert space  $\mathcal{H}$ . Attach to each  $U_i$  a probability  $p_i$  with  $\sum_i p_i = 1$ . Define the functions:

$$\mathcal{G}_W(\rho) := \sum_i p_i U_i^{\otimes k} \rho (U_i^\dagger)^{\otimes k}$$

$$\mathcal{G}_H(\rho) := \int_{\mathbb{U}} U^{\otimes k} \rho (U^\dagger)^{\otimes k} dU$$

for  $\rho \in \mathcal{L}(\mathcal{H}^{\otimes k})$ .  $\mathcal{D}$  is called a unitary  $k$ -design if and only if  $\mathcal{G}_W = \mathcal{G}_H$ .

This implies, that any polynomial of degree  $k$  in the matrix elements of a unitary  $U$  and of degree  $k$  in the matrix elements of  $\bar{U}$  has the same expectation value with respect to the two different probability distribution underlying the expressions for  $\mathcal{G}_W$  and  $\mathcal{G}_H$ . To see this we evaluate the terms  $\langle i_1, \dots, i_k | \mathcal{G}_W(|j_1, \dots, j_k\rangle\langle j'_1, \dots, j'_k|) | i'_1, \dots, i'_k \rangle$  and  $\langle i_1, \dots, i_k | \mathcal{G}_H(|j_1, \dots, j_k\rangle\langle j'_1, \dots, j'_k|) | i'_1, \dots, i'_k \rangle$  and use the defining property of a  $k$ -design  $\mathcal{G}_W = \mathcal{G}_H$  to see that the average of a monomial over  $\mathbb{U}$  and  $\mathcal{D}$  is always the

same. Then any polynomial will also have the same average over  $\mathbb{U}$  and  $\mathcal{D}$ , which justifies the above motivation.

Obviously 2-designs are relevant in our context. In equations (2.12) we integrate over the unitary group. Since the state in the integrand is conjugated by a two-fold tensor product of a unitary, a 2-design would be sufficient to perform the integration. Thus in the statement of the decoupling theorem the integral can be replaced by a 2-design immediately.

**Proposition:** (Decoupling with 2-designs) *Let  $\mathcal{D}$  be a 2-design, let  $\rho_{\text{AR}} \in \mathcal{S}_{\leq}(\mathcal{H}_{\text{A}} \otimes \mathcal{H}_{\text{R}})$  be a sub normalized density operator and let  $\mathcal{T}_{\text{A} \rightarrow \text{E}}$  be a completely positive linear map going from  $\mathcal{S}_{\leq}(\mathcal{H}_{\text{A}} \otimes \mathcal{H}_{\text{R}})$  to  $\mathcal{P}(\mathcal{H}_{\text{E}} \otimes \mathcal{H}_{\text{R}})$  with Choi-Jamiolkowski representation  $\tilde{\omega}_{\text{A}'\text{E}} \in \mathcal{S}_{\leq}(\mathcal{H}_{\text{E}} \otimes \mathcal{H}_{\text{A}'})$ , then*

$$\sum_{U^i \in \mathcal{D}} p_i \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \rho_{\text{AR}} ((U^i_{\text{A}})^{\dagger} \otimes \mathbb{1}_{\text{R}})) - \omega_{\text{E}} \otimes \rho_{\text{R}} \right\|_1 \leq 2^{-\frac{1}{2}H_2(A'|E)_{\omega} - \frac{1}{2}H_2(A|R)_{\rho}}.$$

(We wrote the index  $i$  as a superscript for typographical convenience, which will also be done in the future whenever it simplifies the notation.) The main result of this chapter will be a decoupling formula with  $\varepsilon$ -almost 2-designs. Then the above proposition is an immediate corollary in the case  $\varepsilon = 0$ . For the proof we generalize the derivation of the usual decoupling theorem which only requires the evaluation of expressions involving 2-designs. Therefore although we stated the definition of general  $k$ -designs, for our decoupling results only 2-designs are relevant. We will only consider this special case in the future and refer to this case when we write  $\mathcal{G}_W$  or  $\mathcal{G}_H$ .

## 3.2 Random quantum circuits

A quantum circuit is a sequence of wires and gates. To each wire corresponds some qubit, which is transported through space or time by this wire and to each gate corresponds some unitary operation. A  $k$ -qubit gate takes  $k$  input qubits (i.e.  $k$  wires) and performs some operation on them to give back  $k$  qubits after its application. (I.e. it is given by an element of  $\mathbb{U}(2^k)$ .) Since the wires do not perform any operation it is sufficient to think of the circuit as a sequence of unitaries, that are applied in a certain order:  $W = W_t \cdot \dots \cdot W_2 \cdot W_1$ , where we call  $t$  the time of the circuit. As in the case of classical computation the most common gates are 1 and 2 bit gates. We call

a set of gates *universal* for  $k$ - qubits if any operation which can be performed on  $k$  qubits can be approximated to arbitrary precision using operations from the universal gate set only. A more detailed introduction to the topic of quantum circuits may be found in [14].

Typically quantum computations are modeled using quantum circuits. But for the motivation of our theorem it is also interesting to model the randomization process of a many-particle physical system using quantum circuits. Such approaches were considered in [3] and [7] and here we will keep close to the second one.

There the authors start with a  $k$ -qubit Hilbert space  $\mathcal{H}$  describing some system whose state is given by  $|\psi\rangle$ . In nature the most common type of interaction is a two particle interaction. It corresponds to the application of a 2-qubit unitary gate. Thus a universal gate set of gates in  $\mathbb{U}(4)$  is particularly interesting. A canonical example for such a universal set would be the set of all one qubit gates together with the CNOT gate. The circuit acts in the following way: At each step of the circuit two qubits and an element of the universal gate set are chosen uniformly at random. The gate is applied to the qubits and the circuit proceeds to the next step. Since the gate set is assumed to be universal any element of  $\mathbb{U}(4)$  can be reached. This set is again universal for  $\mathbb{U}(2^k)$ , so that any unitary can be generated by the circuit.

The crucial property of the described circuit is its relation to 2-designs. In the next section we state some related results.

### 3.3 Unitary almost 2-designs

In this section we link the above topics of 2-designs and random circuits by introducing what is called an *almost 2-design*. At the end of this section we state a pivotal theorem, which establishes the fact that random quantum circuits are approximate 2-designs. But first we recapture the definition of the diamond norm of some linear map  $\mathcal{T}_{A \rightarrow E}$  from  $\mathcal{L}(\mathcal{H}_A)$  to  $\mathcal{L}(\mathcal{H}_E)$  [22].

**Definition 7.** Let  $\mathcal{T}_{A \rightarrow E}$  be a linear map from  $\mathcal{L}(\mathcal{H}_A)$  to  $\mathcal{L}(\mathcal{H}_E)$  the diamond norm of  $\mathcal{T}_{A \rightarrow E}$  is defined to be:

$$\|\mathcal{T}_{A \rightarrow E}\|_{\diamond} = \sup_{d_R} \max_{\rho_{AR} \in \mathcal{L}(\mathcal{H}_{AR})} \frac{\|(\mathcal{T}_{A \rightarrow E} \otimes \mathcal{I}_R)(\rho_{AR})\|_1}{\|\rho_{AR}\|_1}$$

If calculated for a difference of two quantum channels, the diamond norm gives the maximum probability of being able to distinguish the two channels experimentally. This is because of the property of the trace distance between two quantum states that

it quantifies how well these states can be distinguished with arbitrary measurements. Thus for two quantum channels  $\mathcal{T}, \mathcal{E}$  the expression

$$\|\mathcal{T} - \mathcal{E}\|_1 := \max_{\rho \in \mathcal{S}(\mathcal{H})} \|\mathcal{T}(\rho) - \mathcal{E}(\rho)\|_1 \quad (3.3)$$

corresponds to the experimental situation, where an optimal input state  $\rho^*$  is chosen and afterwards one tries to distinguish the states  $\mathcal{T}(\rho^*)$  and  $\mathcal{E}(\rho^*)$  with some measurement. But this is still not the best way to distinguish the quantum channels  $\mathcal{T}$  and  $\mathcal{E}$  in an experiment. The definition of  $\|\mathcal{T} - \mathcal{E}\|_1$  does not include the possibility of choosing an initial state in some “larger” Hilbert space. In general one has that

$$\|\mathcal{T} - \mathcal{E}\|_1 \leq \|\mathcal{T} - \mathcal{E}\|_\diamond, \quad (3.4)$$

which motivates the definition of the diamond norm as stated above.

Intuitively an almost 2-design is a finite set of unitary operators which approximates a 2-design. It is a priori not clear which of the many properties a 2-design has, apart from our defining property, should be used for comparison. And once a property is fixed it is also nontrivial to fix the norm in which this approximation should be measured. This results in inconsistent and different definitions in the current literature. We would like to apply the results obtained in [7] for decoupling purposes and therefore abide by their definition.

**Definition 8.** Let  $\mathcal{G}_W$  and  $\mathcal{G}_H$  be as in the definition of the  $k$ -design (Definition 6).  $\mathcal{G}_W$  is called an  $\varepsilon$ -approximate unitary  $k$ -design, if

$$\|\mathcal{G}_W - \mathcal{G}_H\|_\diamond \leq \varepsilon$$

Since the map  $\mathcal{G}_W$  is entirely determined by the set of pairs  $\{(p_i, U_i)\}_{i=1, \dots, n}$ , we sometimes will also refer to that set as the almost 2-design. We now consider the random circuit described above. For infinitely many time-steps the outcome after applying the circuit to some state will be independent of the state on which it is applied. This means that the measure on the set of unitaries reached by the circuit gets unitarily invariant. Since the Haar measure is the unique biinvariant measure on  $\mathbb{U}$ , we can conclude that in the limit of infinite time the distribution of unitaries generated by the circuit reaches the Haar distribution.

Let now  $W$  be a unitary generated by our circuit after  $t$  steps of time. Applying this circuit two times to the different subsystems of a bipartite state  $\rho_{AB}$  gives a state  $\rho_{AB}^W = W \otimes W \rho_{AB} W^\dagger \otimes W^\dagger$ . If the average of all the  $\rho_{AB}^W$  taken over the different

circuits  $W$  equals the average calculated over  $\mathbb{U}$  with respect to the Haar measure, we say that the random circuits constitute a 2-design. Unfortunately it turns out that the convergence rate of the random circuits towards the Haar distribution is exponentially slow in the number of qubits of the underlying system [7], [3], [14]. Nevertheless, the authors of [7] (Theorems 9 and 10) derive the following pivotal theorem:

**Theorem:** (Random quantum circuits are approximate 2-designs) *Let  $\mu$  be the probability distribution corresponding to any universal gate set on  $\mathbb{U}(4)$  and let  $W$  be a random circuit on  $n$  qubits obtained by drawing  $t$  random unitaries according to  $\mu$  and applying each of them to a random pair of qubits. Then there exists  $C$  and ( $C = C(\mu)$  only) such that for any  $\varepsilon > 0$  and any  $t \geq C(n^2 + n \log(1/\varepsilon))$ ,  $\mathcal{G}_W$  is an  $\varepsilon$ -approximate unitary 2-design.*

This theorem implies that random two particle interactions as described above yield approximate 2-designs. We would like to understand, if the process is really decoupling in the sense that if it occurs on some system it destroys the correlations to its reference system. This is relevant from a physical point of view, because as already mentioned the time until the random circuits get close to being distributed with respect to Haar measure and thus the time until the usual decoupling theorem is applicable is exponentially large. So what happens with the system in the physical situation after polynomial circuit time? We consider a decoupling theorem with almost 2-designs.

### 3.4 Decoupling with almost 2-designs

In this section we formulate and prove the core theorem of this chapter. It generalizes the usual decoupling theorem in the sense that it is valid in the case where almost 2-designs are considered.

**Theorem:** (Decoupling with  $\varepsilon$ -approximate unitary 2-designs) *Let  $\rho_{\text{AR}} \in \mathcal{S}_{\leq}(\mathcal{H}_{\text{A}} \otimes \mathcal{H}_{\text{R}})$  be a sub normalized density operator and let  $\mathcal{T}_{\text{A} \rightarrow \text{E}}$  be a completely positive, linear map going from  $\mathcal{S}_{\leq}(\mathcal{H}_{\text{A}} \otimes \mathcal{H}_{\text{R}})$  to  $\mathcal{P}(\mathcal{H}_{\text{E}} \otimes \mathcal{H}_{\text{R}})$  with Choi-Jamiołkowski*

representation  $\omega_{A'E} \in \mathcal{S}_{\leq}(\mathcal{H}_E \otimes \mathcal{H}_{A'})$ , then

$$\begin{aligned} & \sum_{(p_i, U_i) \in \mathcal{D}} p_i \left\| \mathcal{T}((U_A^i \otimes \mathbb{1}_R) \rho_{AR} ((U_A^i)^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\|_1 \\ & \leq \sqrt{1 + 4\varepsilon d_A^4} 2^{-\frac{1}{2}(H_2(A'|E)_\omega + H_2(A|R)_\rho)} \end{aligned}$$

where the summation goes over pairs  $(p_i, U_i)$ , such that  $\mathcal{D}$  constitutes an  $\varepsilon$ -approximate 2-design.

For a proof we proceed similarly to the proof of the decoupling theorem in the last chapter. Like before, we introduce the map  $\mathcal{E}_{\bar{A} \rightarrow E}$  which we define to be the unique Choi-Jamiolkowski preimage of the state  $\rho_{AR}$  and write for any  $i$ :

$$\begin{aligned} & \mathcal{T}((U_A^i \otimes \mathbb{1}_R) \rho_{AR} (U_A^{i\dagger} \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \\ & = (\mathcal{T} \otimes \mathcal{E})((U_A^i \otimes \mathbb{1}_{\bar{A}})(\xi_{A\bar{A}})(U_A^{i\dagger} \otimes \mathbb{1}_{\bar{A}})), \end{aligned} \quad (3.5)$$

where  $\xi_{A\bar{A}} = \Phi_{A\bar{A}} - \pi_A \otimes \pi_{\bar{A}}$  is the decoupling state.

The idea of the derivation is to add and subtract an integral term which is "close" to the sum at a step where this is convenient and then use the defining property of the almost 2-design.

To go from the difficult Schatten 1-norm of the theorem to the manageable Schatten 2-norm we use Hölder inequality as stated in Appendix A (or *Lemma 5*, [19]) in exactly the same manner as it was done in the last chapter for the proof of the decoupling theorem. Again we introduce positive semidefinite, normalized operators  $\sigma_E$  and  $\zeta_R$  and the maps  $\tilde{\mathcal{T}}$  and  $\tilde{\mathcal{E}}$  with

$$\tilde{\mathcal{T}}(\tau_{A\bar{A}}) := (\sigma_E \otimes \mathbb{1}_{\bar{A}})^{-1/4} \mathcal{T}(\tau_{A\bar{A}}) (\sigma_E \otimes \mathbb{1}_{\bar{A}})^{-1/4} \quad \forall \tau_{A\bar{A}} \in \mathcal{L}(\mathcal{H}_{A\bar{A}}) \quad (3.6)$$

$$\tilde{\mathcal{E}}(\tau_{A\bar{A}}) := (\mathbb{1}_A \otimes \zeta_R)^{-1/4} \mathcal{E}(\tau_{A\bar{A}}) (\mathbb{1}_A \otimes \zeta_R)^{-1/4} \quad \forall \tau_{A\bar{A}} \in \mathcal{L}(\mathcal{H}_{A\bar{A}}) \quad (3.7)$$

and find

$$\begin{aligned} & \left\| (\mathcal{T} \otimes \mathcal{E})((U_A^i \otimes \mathbb{1}_{\bar{A}})(\xi_{A\bar{A}})(U_A^{i\dagger} \otimes \mathbb{1}_{\bar{A}})) \right\|_1 \\ & \leq \left\| (\tilde{\mathcal{T}} \otimes \tilde{\mathcal{E}})((U_A^i \otimes \mathbb{1}_{\bar{A}})(\xi_{A\bar{A}})(U_A^{i\dagger} \otimes \mathbb{1}_{\bar{A}})) \right\|_2 \end{aligned} \quad (3.8)$$

$$= \sqrt{\text{tr} \left( (\tilde{\mathcal{T}} \otimes \tilde{\mathcal{E}})(U_A^i \otimes \mathbb{1}_{\bar{A}})(\xi_{A\bar{A}}) U_A^{i\dagger} \otimes \mathbb{1}_{\bar{A}} \right)^2}. \quad (3.9)$$

The next step is to apply the swap trick (Appendix C) as was already done in the proof of the usual decoupling theorem. This gives

$$\begin{aligned} & \sqrt{\text{tr} \left( (\tilde{\mathcal{T}} \otimes \tilde{\mathcal{E}}) (U_{\mathbf{A}}^i \otimes \mathbb{1}_{\tilde{\mathbf{A}}} \xi_{\mathbf{A}\tilde{\mathbf{A}}} U_{\mathbf{A}}^{i\dagger} \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^2 \right)} \\ &= \sqrt{\text{tr} \left( (\tilde{\mathcal{T}} \otimes \tilde{\mathcal{E}})^{\otimes 2} \left( (U_{\mathbf{A}}^i \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} (U_{\mathbf{A}}^{i\dagger} \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} \right) \mathcal{F}_{\mathbf{E}} \otimes \mathcal{F}_{\mathbf{R}} \right)} \end{aligned} \quad (3.10)$$

$$= \sqrt{\text{tr} \left( \left( (U_{\mathbf{A}}^i \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} (U_{\mathbf{A}}^{i\dagger} \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} \right) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{E}}] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{R}}] \right)}. \quad (3.11)$$

In order to deal with the square root we use Jensen inequality, which gives

$$\begin{aligned} & \sum_i p_i \sqrt{\text{tr} \left( \left( (U_{\mathbf{A}}^i \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} (U_{\mathbf{A}}^{i\dagger} \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} \right) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{E}}] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{R}}] \right)} \\ & \leq \sqrt{\sum_i p_i \text{tr} \left( \left( (U_{\mathbf{A}}^i \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} (U_{\mathbf{A}}^{i\dagger} \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} \right) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{E}}] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{R}}] \right)} \end{aligned} \quad (3.12)$$

$$= \sqrt{\text{tr} \left( \left( \sum_i p_i (U_{\mathbf{A}}^i \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} (U_{\mathbf{A}}^{i\dagger} \otimes \mathbb{1}_{\tilde{\mathbf{A}}})^{\otimes 2} \right) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{E}}] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{R}}] \right)} \quad (3.13)$$

$$= \sqrt{\text{tr} \left( \left( \sum_i p_i (U_{\mathbf{A}}^{i\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} ((U_{\mathbf{A}}^{i\dagger})^{\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) \right) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{E}}] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2} [\mathcal{F}_{\mathbf{R}}] \right)}. \quad (3.14)$$

To apply the defining property of the almost 2-design we need to compare the term  $\sum_i p_i (U_{\mathbf{A}}^{i\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} ((U_{\mathbf{A}}^{i\dagger})^{\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2})$  with the corresponding integral. We therefore add  $\int (U_{\mathbf{A}}^{\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} ((U_{\mathbf{A}}^\dagger)^{\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) dU$  to the argument of the square root and subtract it again. Note that we have the following two relations:

$$\sum_i p_i (U_{\mathbf{A}}^{i\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} ((U_{\mathbf{A}}^{i\dagger})^{\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) = (\mathcal{G}_W \otimes \mathcal{I}_{\tilde{\mathbf{A}}\tilde{\mathbf{A}}'}) (\xi_{\mathbf{A}\tilde{\mathbf{A}}}^{\otimes 2}), \quad (3.15)$$

$$\int (U_{\mathbf{A}}^{\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) (\xi_{\mathbf{A}\tilde{\mathbf{A}}})^{\otimes 2} ((U_{\mathbf{A}}^\dagger)^{\otimes 2} \otimes \mathbb{1}_{\tilde{\mathbf{A}}}^{\otimes 2}) dU = (\mathcal{G}_H \otimes \mathcal{I}_{\tilde{\mathbf{A}}\tilde{\mathbf{A}}'}) (\xi_{\mathbf{A}\tilde{\mathbf{A}}}^{\otimes 2}). \quad (3.16)$$

Where the  $\mathcal{G}_W$  and  $\mathcal{G}_H$  are as in Definition 6 for  $k = 2$  and  $\mathcal{I}_{\tilde{\mathbf{A}}\tilde{\mathbf{A}}'}$  denotes the operator identity on  $\tilde{\mathbf{A}}\tilde{\mathbf{A}}'$ . The above evidently would be valid if there were no correlations between the systems  $\mathbf{A}$ ,  $\mathbf{A}'$ ,  $\tilde{\mathbf{A}}$  and  $\tilde{\mathbf{A}}'$  (which is not true for  $\xi_{\mathbf{A}\tilde{\mathbf{A}}}$ ). But by linearity of all the considered maps the statements also follow for  $\xi_{\mathbf{A}\tilde{\mathbf{A}}}$ . For notational convenience

we drop the square root in equation (3.14) and consider its argument only. We have:

$$\begin{aligned} & \text{tr} \left( \left( \sum_i p_i (U_A^{i \otimes 2} \otimes \mathbb{1}_{\bar{A}}^{\otimes 2}) (\xi_{A\bar{A}}^{\otimes 2}) ((U_A^{i \dagger})^{\otimes 2} \otimes \mathbb{1}_{\bar{A}}^{\otimes 2}) \right) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right) \\ &= \text{tr} \left( ((\mathcal{G}_W \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2})) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right) \\ & \quad + \text{tr} \left( (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right) \end{aligned} \quad (3.17)$$

$$\begin{aligned} & \leq \left\| ((\mathcal{G}_W \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2})) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right\|_1 \\ & \quad + \text{tr} \left( (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right) \end{aligned} \quad (3.18)$$

The inequality is by the fact that the trace is given by the sum of the eigenvalues of some matrix in contrast to the Schatten 1-norm which is given by the sum of the absolute values of the eigenvalues. Thus the Schatten 1-norm of a matrix is always an upper bound on its trace.

The second term of equation (3.18) is calculated in an analogous way as in the proof of the original decoupling theorem. We postpone its evaluation to the end of our proof and first consider the term with the Schatten 1-norm. This term can be upper bounded with an application of *Lemma 2*. We apply

$$\|ABC\|_1 \leq \|A\|_\infty \|B\|_1 \|C\|_\infty \quad (3.19)$$

with  $A = \mathbb{1}_{A\bar{A}, \bar{A}\bar{A}}$  and find

$$\begin{aligned} & \left\| ((\mathcal{G}_W \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2})) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right\|_1 \\ & \leq \left\| ((\mathcal{G}_W \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2})) \right\|_1 \left\| (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right\|_\infty \end{aligned} \quad (3.20)$$

$$= \left\| ((\mathcal{G}_W \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2})) \right\|_1 \left\| (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \right\|_\infty \left\| (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right\|_\infty. \quad (3.21)$$

The last equality is by the fact the the absolute value of the biggest eigenvalue of the tensor product is just the product of the absolute values of the biggest eigenvalues of the two components. By the definition of the  $\varepsilon$ -almost 2-design and the definition of the diamond norm we have:

$$\varepsilon \geq \|\mathcal{G}_W - \mathcal{G}_H\|_\diamond \quad (3.22)$$

$$:= \sup_{d_R} \max_{\rho_{AR} \in \mathcal{L}(\mathcal{H}_{AR})} \frac{\|(\mathcal{G}_W \otimes \mathcal{I}_R)(\rho_{AR}) - (\mathcal{G}_H \otimes \mathcal{I}_R)(\rho_{AR})\|_1}{\|\rho_{AR}\|_1} \quad (3.23)$$

$$\geq \frac{\left\| ((\mathcal{G}_W \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2})) \right\|_1}{\left\| \xi_{A\bar{A}}^{\otimes 2} \right\|_1} \quad (3.24)$$

$$\geq \frac{1}{4} \left\| ((\mathcal{G}_W \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}})(\xi_{A\bar{A}}^{\otimes 2})) \right\|_1 \quad (3.25)$$



Inequality (3.25) can be seen using the evident fact that  $\|\xi_{AA}^{\otimes 2}\|_1 = \|\xi_{AA}\|_1^2$  and by plugging in the definition  $\xi_{AA} := \Phi_{AA} - \pi_A \otimes \pi_A$  into this expression. Using (3.25) we obtain an upper bound for (3.21):

$$\left\| ((\mathcal{G}_W \otimes \mathcal{I}_{\bar{A}\bar{A}'})(\xi_{AA}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\bar{A}\bar{A}'})(\xi_{AA}^{\otimes 2})) \right\|_1 \left\| (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \right\|_\infty \left\| (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right\|_\infty \quad (3.26)$$

$$\leq 4\varepsilon \left\| (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \right\|_\infty \left\| (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right\|_\infty \quad (3.27)$$

Note that both terms with norms look almost identical so it is sufficient to find an upper bound for one of them only. We analyze the first term  $\|(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E]\|_\infty$ . Let  $P_{AA}^+$  be the projector corresponding to the biggest absolute eigenvalue of  $(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E]$ . Then the  $\infty$ -norm can be rewritten in the following way:

$$\left\| (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \right\|_\infty = \text{tr} \left( P_{AA}^+ (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \right) \quad (3.28)$$

$$= \text{tr} \left( (\tilde{\mathcal{T}})^{\otimes 2}[P_{AA}^+]\mathcal{F}_E \right) \quad (3.29)$$

To be able to apply the swap trick and thus get rid of the operator  $\mathcal{F}_E$ , we need to decompose  $P_{AA}^+$  into some basis:  $P_{AA}^+ = \sum_{i,j} c_{ij} \sigma_i^A \otimes \sigma_j^{A'}$ . Without loss of generality we choose the coefficients  $c_{ij}$  to be real. (For example,  $\{\sigma_i^A\}_{i=1,\dots,d_A}$  might be an orthonormal basis of the space  $\mathcal{L}^\dagger(\mathcal{H}_A)$ .) This gives:

$$\text{tr} \left( (\tilde{\mathcal{T}})^{\otimes 2}[P_{AA}^+]\mathcal{F}_E \right) \quad (3.30)$$

$$= \sum_{i,j} c_{ij} \text{tr} \left( (\tilde{\mathcal{T}}(\sigma_i^A) \otimes \tilde{\mathcal{T}}(\sigma_j^{A'}))\mathcal{F}_E \right) \quad (3.31)$$

$$= \sum_{i,j} c_{ij} \text{tr} \left( \tilde{\mathcal{T}}(\sigma_i^A) \tilde{\mathcal{T}}(\sigma_j^{A'}) \right) \quad (3.32)$$

We rewrite  $\tilde{\mathcal{T}}(\sigma_i^A)$  using its Choi-Jamiolkowski representation.

$$\sum_{i,j} c_{ij} \text{tr} \left( (\tilde{\mathcal{T}}(\sigma_i^A) \tilde{\mathcal{T}}(\sigma_j^{A'})) \right) = d_A^2 \sum_{i,j} c_{ij} \text{tr} \left( \text{tr}_A (\tilde{\omega}_{AE} \mathbf{1}_E \otimes \sigma_i^{i\top}) \text{tr}_{A'} (\tilde{\omega}_{A'E} \mathbf{1}_E \otimes \sigma_j^{j\top}) \right) \quad (3.33)$$

$$= d_A^2 \sum_{i,j} c_{ij} \text{tr} \left( (\mathbf{1}_{A'} \otimes (\tilde{\omega}_{AE} \mathbf{1}_E \otimes \sigma_i^{i\top})) \mathbf{1}_A \otimes (\tilde{\omega}_{A'E} \mathbf{1}_E \otimes \sigma_j^{j\top}) \right) \quad (3.34)$$

$$= d_A^2 \sum_{i,j} c_{ij} \text{tr} \left( (\mathbf{1}_{A'} \otimes \tilde{\omega}_{AE}) (\mathbf{1}_A \otimes \tilde{\omega}_{A'E}) (\mathbf{1}_E \otimes \sigma_i^{i\top} \otimes \sigma_j^{j\top}) \right) \quad (3.35)$$

$$= d_A^2 \text{tr} \left( (\mathbf{1}_{A'} \otimes \tilde{\omega}_{AE}) (\mathbf{1}_A \otimes \tilde{\omega}_{A'E}) (\mathbf{1}_E \otimes (P_{AA}^+)^{\top}) \right) \quad (3.36)$$

Untill now no inequalities were used and the calculation following equation (3.28) is still exact. We need to find the entropies again. For this we introduce a basis  $\{\sigma_i^A\}_{i=1,\dots,d_A}$  for  $\mathcal{L}^\dagger(\mathcal{H}_A)$  and a basis  $\{\sigma_i^E\}_{i=1,\dots,d_E}$  for  $\mathcal{L}^\dagger(\mathcal{H}_E)$ . Moreover we choose them to be orthonormal with respect to the scalar product:

$$\langle \mu_X | \nu_X \rangle_{\mathcal{L}^\dagger(\mathcal{H}_X)} := \frac{1}{d_X} \text{tr}(\mu_X \cdot \nu_X) \quad \forall \mu_X, \nu_X \in \mathcal{L}^\dagger(\mathcal{H}_X) \quad (3.37)$$

i. e. we have

$$\frac{1}{d_A} \text{tr}(\sigma_i^A \sigma_j^A) = \delta_{ij}. \quad (3.38)$$

Now the product states  $\{\sigma_i^A \otimes \sigma_j^E\}_{i=1,\dots,d_A; j=1,\dots,d_E}$  form an orthonormal basis for  $\mathcal{L}^\dagger(\mathcal{H}_{AE})$  with respect to the scalar product introduced in equation (3.37):

$$\frac{1}{d_A d_E} \text{tr}(\sigma_i^A \otimes \sigma_j^E \sigma_k^A \otimes \sigma_l^E) = \frac{1}{d_A} \text{tr}(\sigma_i^A \sigma_k^A) \cdot \frac{1}{d_E} \text{tr}(\sigma_j^E \sigma_l^E) \quad (3.39)$$

$$= \delta_{ik} \delta_{jl} \quad (3.40)$$

We now write the states  $\tilde{\omega}_{AE}$ ,  $\tilde{\omega}_{A'E}$  and  $(P_{AA'}^+)^T$  in that basis:

$$\tilde{\omega}_{AE} := \sum_{i,j} a_{ij} \sigma_i^A \otimes \sigma_j^E \quad \wedge \quad a_{ij} := \frac{1}{d_A d_E} \text{tr}(\sigma_i^A \otimes \sigma_j^E \tilde{\omega}_{AE}) \quad (3.41)$$

$$\tilde{\omega}_{A'E} := \sum_{i,j} a_{ij} \sigma_i^{A'} \otimes \sigma_j^E \quad \wedge \quad a_{ij} := \frac{1}{d_A d_E} \text{tr}(\sigma_i^{A'} \otimes \sigma_j^E \tilde{\omega}_{A'E}) \quad (3.42)$$

$$(P_{AA'}^+)^T := \sum_{i,j} c_{ij} \sigma_i^A \otimes \sigma_j^{A'} \quad \wedge \quad c_{ij} := \frac{1}{d_A d_A} \text{tr}(\sigma_i^A \otimes \sigma_j^{A'} (P_{AA'}^+)^T) \quad (3.43)$$

Since all matrices in the above statements are hermitian the coefficients  $a_{ij}$  and  $c_{ij}$  are real. Moreover the coefficients in the expansion of  $\tilde{\omega}_{AE}$  and  $\tilde{\omega}_{A'E}$  are the same, because the corresponding matrices are the same. Plugging in the expansions into equation (3.36) yields:

$$d_A^2 \text{tr}(\mathbb{1}_{A'} \otimes \tilde{\omega}_{AE} \mathbb{1}_A \otimes \tilde{\omega}_{A'E} \mathbb{1}_E \otimes (P_{AA'}^+)^T) \quad (3.44)$$

$$= d_A^2 \sum_{i,j,k,l,m,n} a_{ij} a_{kl} c_{mn} \text{tr}(\mathbb{1}_{A'} \otimes \sigma_i^A \otimes \sigma_j^E \mathbb{1}_A \otimes \sigma_k^{A'} \otimes \sigma_l^E \mathbb{1}_E \otimes \sigma_m^A \otimes \sigma_n^{A'}) \quad (3.45)$$

$$= d_A^2 \sum_{i,j,k,l,m,n} a_{ij} a_{kl} c_{mn} \text{tr}(\sigma_i^A \sigma_m^A) \text{tr}(\sigma_k^{A'} \sigma_n^{A'}) \text{tr}(\sigma_j^E \sigma_l^E) \quad (3.46)$$

$$= d_A^4 d_E \sum_{i,j,k,l,m,n} a_{ij} a_{kl} c_{mn} \delta_{im} \delta_{kn} \delta_{jl} \quad (3.47)$$

$$= d_A^4 d_E \sum_{i,j,k} a_{ij} a_{kj} c_{ik} \quad (3.48)$$

We now introduce the matrices:

$$A := (a_{ij}) \quad (3.49)$$

$$C := (c_{ij}) \quad (3.50)$$

By the definition of the transpose of a matrix we have:  $A^\top := (a_{ji})$  for  $A$  defined as above. Then (3.48) becomes:

$$d_A^4 d_E \sum_{i,j,k} a_{ij} a_{kj} c_{ik} = d_A^4 d_E \text{tr}(A^\top C A) \quad (3.51)$$

$$= d_A^4 d_E \text{tr}(A A^\top C) \quad (3.52)$$

$$\leq d_A^4 d_E \|A A^\top C\|_1 \quad (3.53)$$

$$= d_A^4 d_E \|A A^\dagger C\|_1 \quad (3.54)$$

$$\leq d_A^4 d_E \|A A^\dagger\|_1 \|C\|_\infty \quad (3.55)$$

$$\leq d_A^4 d_E \|A A^\dagger\|_1 \|C\|_2 \quad (3.56)$$

$$= d_A^4 d_E \text{tr}(A A^\dagger) \|C\|_F \quad (3.57)$$

The replacement of the transpose of  $A$  with the hermitian conjugate  $A^\dagger$  in (3.54) is possible because of the fact that all entries of  $A$  are real. In equation (3.57) we rewrote the Schatten 2-norm in terms of the Frobenius norm  $\|C\|_F = \sqrt{\sum_{ij} |c_{ij}|^2}$  [1] and used the fact that all eigenvalues of  $A A^\dagger$  are real and positive. Using the explicit formula for the coefficients  $c_{ij}$  we calculate the Frobenius norm of  $C$ , where we use that all of its entries are real.

$$\|C\|_F^2 = \sum_{ij} |c_{ij}|^2 \quad (3.58)$$

$$= \sum_{ij} c_{ij}^2 \quad (3.59)$$

$$= \frac{1}{d_A^4} \sum_{ij} \text{tr} \left( \sigma_i^A \otimes \sigma_j^{A'} (P_{AA'}^+)^{\top} \right) \text{tr} \left( \sigma_i^A \otimes \sigma_j^{A'} (P_{AA'}^+)^{\top} \right) \quad (3.60)$$

$$= \frac{1}{d_A^4} \text{tr} \left( \left( \sum_{ij} \text{tr} \left( \sigma_i^A \otimes \sigma_j^{A'} (P_{AA'}^+)^{\top} \right) \sigma_i^A \otimes \sigma_j^{A'} \right) (P_{AA'}^+)^{\top} \right) \quad (3.61)$$

$$= \frac{1}{d_A^2} \text{tr} \left( (P_{AA'}^+)^{\top} (P_{AA'}^+)^{\top} \right) \quad (3.62)$$

$$= \frac{1}{d_A^2} \text{tr} \left( (P_{AA'}^+)^{\top} \right) \quad (3.63)$$

$$= \frac{1}{d_A^2} \quad (3.64)$$

So we have

$$\|C\|_F = \frac{1}{d_A}. \quad (3.65)$$

In equation (3.63) the fact that  $(P_{AA'}^+)^\top$  is a projector was used. And in equation (3.64) we exhibited the fact that  $(P_{AA'}^+)^\top$  corresponds to some fixed eigenvalue of  $(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E]$  and therefore has eigenvalues which are all zero beside one which is one.

The trace term in (3.57) can be calculated similarly. We use the explicit formula for the coefficients:

$$\text{tr}(AA^\dagger) = \sum_{ij} a_{ij} a_{ij} \quad (3.66)$$

$$= \frac{1}{d_A^2 d_E^2} \sum_{ij} \text{tr}(\sigma_i^A \otimes \sigma_j^E \tilde{\omega}_{A'E}) \text{tr}(\sigma_i^A \otimes \sigma_j^E \tilde{\omega}_{A'E}) \quad (3.67)$$

$$= \frac{1}{d_A^2 d_E^2} \text{tr} \left( \left( \sum_{ij} \text{tr}(\sigma_i^A \otimes \sigma_j^E \tilde{\omega}_{A'E}) \sigma_i^A \otimes \sigma_j^E \right) \tilde{\omega}_{A'E} \right) \quad (3.68)$$

$$= \frac{1}{d_A d_E} \text{tr}(\tilde{\omega}_{A'E}^2) \quad (3.69)$$

Plugging this expression together with (3.65) into equation (3.57) yields:

$$d_A^4 d_E \sum_{i,j,k} a_{ij} a_{kj} c_{ik} \leq d_A^2 \text{tr}(\tilde{\omega}_{A'E}^2), \quad (3.70)$$

and with it the desired upper bound for  $\left\| (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \right\|_\infty$ :

$$\left\| (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \right\|_\infty \leq d_A^2 \text{tr}(\tilde{\omega}_{A'E}^2). \quad (3.71)$$

An identical calculation reveals that

$$\left\| (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right\|_\infty \leq d_A^2 \text{tr}(\tilde{\rho}_{AR}^2). \quad (3.72)$$

Thus we finally obtain the bound for (3.18) using (3.27):

$$\begin{aligned} & \left\| ((\mathcal{G}_W \otimes \mathcal{I}_{\tilde{A}\tilde{A}'})(\xi_{AA}^{\otimes 2}) - (\mathcal{G}_H \otimes \mathcal{I}_{\tilde{A}\tilde{A}'})(\xi_{AA}^{\otimes 2})) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right\|_1 \\ & \leq 4\varepsilon d_A^4 \text{tr}(\tilde{\omega}_{A'E}^2) \text{tr}(\tilde{\rho}_{AR}^2) \end{aligned} \quad (3.73)$$

The only thing left to do is to evaluate the trace term in (3.18) but this is equivalent to proving the usual decoupling theorem in the way it was done in chapter 2. We

have in accordance with the steps following (2.11) to (2.40):

$$\begin{aligned} & \text{tr} \left( (\mathcal{G}_H \otimes \mathcal{I}_{\tilde{A}\tilde{A}}) (\xi_{\tilde{A}\tilde{A}}^{\otimes 2}) (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} [\mathcal{F}_E] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2} [\mathcal{F}_R] \right) \\ &= \text{tr} \left( (\xi_{\tilde{A}\tilde{A}}^{\otimes 2}) \int [(U_A)^\dagger]^{\otimes 2} (\tilde{\mathcal{T}}^\dagger)^{\otimes 2} [\mathcal{F}_E] (U_A)^{\otimes 2} dU \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2} [\mathcal{F}_R] \right) \end{aligned} \quad (3.74)$$

$$\leq \frac{1}{\text{tr}[\omega_{A'E}]} \text{tr} \left( ((\sigma_E^{-1/2} \otimes \mathbb{1}_{A'}) \omega_{A'E})^2 \right) \frac{1}{\text{tr}[\rho_{AR}]} \text{tr} \left( ((\mathbb{1}_A \otimes \zeta_R^{-1/2}) \rho_{AR})^2 \right) \quad (3.75)$$

Adjusting the operators  $\sigma_E$  and  $\zeta_R$  in a way such that the above expressions correspond to  $H_2$ -entropies, we could recapture after taking the square root and applying Jensen's inequality the decoupling theorem.

Here, we are interested in decoupling with almost 2-designs and thus we need to consider the first term of (3.18), too. Taking the obtained upper bounds on the two terms together with the correct adjustment of  $\sigma_E$  and  $\zeta_R$  yields

$$\begin{aligned} & \sum_i p_i \left\| \mathcal{T}((U_A^i \otimes \mathbb{1}_R) \rho_{AR} (U_A^{i\dagger} \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\|_1 \\ & \leq \sqrt{2^{-H_2(A'|E)_\omega - H_2(A|R)_\rho} + 4\varepsilon d_A^4 2^{-H_2(A'|E)_\omega - H_2(A|R)_\rho}} \end{aligned} \quad (3.76)$$

$$= \sqrt{1 + 4\varepsilon d_A^4} 2^{-\frac{1}{2}(H_2(A'|E)_\omega + H_2(A|R)_\rho)}, \quad (3.77)$$

which concludes the proof of the decoupling theorem with almost 2-designs.

### 3.5 Analysis of the decoupling formula

In this section we would like to shortly go back to our original motivation and analyze whether the discussed circuits do well in the sense of decoupling. From the fact that quantum circuits constitute approximate 2-designs we already now that in a many qubit system with dynamics described with the above quantum circuit, the different possible unitary evolutions are given by elements of an almost 2-designs. Since typical dynamics in nature are given by local two particle interactions and the corresponding circuits (as discussed in [3]) are of the above type (but less general), we conclude that our model can roughly be used to describe the internal dynamics of a many qubit system. Moreover we know that in order to reach an  $\varepsilon$ -almost 2-design we need at least  $t \geq C(n^2 + n \log \frac{1}{\varepsilon})$  time steps in the circuit, with  $C$  being some constant that only depends on the concrete circuit used.

To say that some process occurring on the system is “decoupling” we need to be sure that the required unitary is reached by the circuit in polynomial time only. This is certainly not true for any unitary with distribution according to Haar measure and

thus the original decoupling theorem cannot be used to make a statement about this question. In contrast the derived decoupling formula states that there exists some process  $W$  on the system that reaches decoupling in the sense that

$$\left\| \mathcal{T}((W_A \otimes \mathbb{1}_R) \rho_{AR} (W_A^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \right\|_1 \leq \sqrt{1 + 4\varepsilon d_A^4} 2^{-\frac{1}{2} (H_2(A|E)_\omega + H_2(A|R)_\rho)}. \quad (3.78)$$

This formula implies that the time that one has to wait until one reaches a certain quality of decoupling does not depend on the dimensions of the reference system  $R$  and the output system  $E$  of the channel  $\mathcal{T}$ . Note, moreover, that the factor  $d_A^4$  does not significantly increase the time that is required until decoupling is reached. To reach an  $\bar{\varepsilon}$ -approximate 2-design with  $\bar{\varepsilon} := \frac{\varepsilon}{d_A^4}$  the circuit requires at least a time  $\bar{t}$  with  $\bar{t}$  given by:

$$\bar{t} = C \left( n^2 + n \log \left( \frac{d_A^4}{\varepsilon} \right) \right) \quad (3.79)$$

$$= C \left( n^2 + n \log \left( \frac{2^{4n}}{\varepsilon} \right) \right) \quad (3.80)$$

Assuming that  $t$  is the minimum time required for the circuit to reach an  $\varepsilon$ -almost 2-design a short calculation reveals:

$$\bar{t} = C \left( n^2 + 4n^2 + n \log \left( \frac{1}{\varepsilon} \right) \right) \quad (3.81)$$

$$\leq C \left( 5n^2 + 5n \log \left( \frac{1}{\varepsilon} \right) \right) \quad (3.82)$$

$$= 5t \quad (3.83)$$

This means that once the circuit has reached an  $\varepsilon$ -almost 2-design, one has to wait only five times longer until the circuits form an  $\bar{\varepsilon}$ -almost 2-design. This additional time certainly does not affect the physical realizability of the required unitary evolution.

## Chapter 4

# A smoothed version of the decoupling formula for $\varepsilon$ -almost 2-designs

As in the case of the original Decoupling Theorem, we would like to obtain a smoothed version of the decoupling formula with almost 2-designs i.e. we would like to replace the occurring  $H_2$ -entropies using smooth  $H_{\min}$ -entropies. This is done conceptually in exactly the same way in both cases. We therefore keep our discussions short and refer to [19] Chapter 3. First we rewrite the formula for almost 2-designs using the fact that  $H_{\min}(A|B)_\rho \leq H_2(A|B)_\rho$  and then we use the unsmoothed formula to find its smoothed counterpart.

**Theorem:** (Smoothed decoupling formula for  $\varepsilon$ -approximate 2-designs) *Let  $\rho_{AR} \in \mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_R)$  be a sub normalized density operator and let  $\mathcal{T}_{A \rightarrow E}$  be a completely positive linear map going from  $\mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_R)$  to  $\mathcal{P}(\mathcal{H}_E \otimes \mathcal{H}_R)$  with Choi-Jamiołkowski representation  $\omega_{A'E} \in \mathcal{S}_{\leq}(\mathcal{H}_E \otimes \mathcal{H}_{A'})$  and let  $\delta > 0$  be small enough, then*

$$\begin{aligned} \sum_{(p_i, U_i) \in \mathcal{D}} p_i \left\| \mathcal{T}((U_A^i \otimes \mathbb{1}_R) \rho_{AR} ((U_A^i)^\dagger \otimes \mathbb{1}_R)) - \omega_{A'E} \otimes \rho_R \right\|_1 \\ \leq \sqrt{1 + 4\varepsilon d_A^4} 2^{-\frac{1}{2} H_{\min}^\delta(A'|E)_\omega - \frac{1}{2} H_{\min}^\delta(A|R)_\rho} + 8d_A \varepsilon \delta + 12\delta \end{aligned}$$

where the summation goes over pairs  $(p_i, U_i)$ , such that  $\mathcal{D}$  constitutes an  $\varepsilon$ -approximate 2-design.

For the proof let us introduce the state  $\hat{\omega}_{A'E} \in \mathcal{S}_{\leq}(\mathcal{H}_{A'E})$  (which we sometimes denote shortly as  $\hat{\omega}$ ) with the properties  $\bar{P}(\omega_{A'E}, \hat{\omega}_{A'E}) \leq \delta$  and  $H_{\min}(A'|E)_{\hat{\omega}} = H_{\min}^\delta(A'|E)_\omega$ . This state hits the bound in the definition of  $H_{\min}^\delta$  i.e. it maximizes  $H_{\min}(A'|E)$

over  $\mathcal{B}^\delta(\omega)$ . Analogously  $\hat{\rho}_{\text{AR}}$  is defined to be an operator with  $\bar{P}(\hat{\rho}_{\text{AR}}, \rho_{\text{AR}}) \leq \delta$  and  $H_{\min}(\text{A}|\text{R})_{\hat{\rho}} = H_{\min}^\delta(\text{A}|\text{R})_{\rho}$ .

Using the generalized Fuchs- van der Graaf inequalities (as in [19] Chapter 3) we find that:

$$\|\omega_{\text{A}'\text{E}} - \hat{\omega}_{\text{A}'\text{E}}\|_1 \leq 2\delta \quad \wedge \quad \|\rho_{\text{AR}} - \hat{\rho}_{\text{AR}}\|_1 \leq 2\delta \quad (4.1)$$

Now we decompose  $\hat{\omega} - \omega$  and  $\hat{\rho} - \rho$  into positive operators with orthogonal support. We write

$$\hat{\omega} - \omega = \Delta_+ - \Delta_- \quad \wedge \quad \hat{\rho} - \rho = \Gamma_+ - \Gamma_- \quad (4.2)$$

and conclude from (4.1) that

$$\|\Delta_+\|_1 \leq 2\delta \quad \wedge \quad \|\Delta_-\|_1 \leq 2\delta \quad \wedge \quad \|\Gamma_+\|_1 \leq 2\delta \quad \wedge \quad \|\Gamma_-\|_1 \leq 2\delta. \quad (4.3)$$

Moreover we introduce the completely positive maps  $\hat{\mathcal{T}}$ ,  $\mathcal{D}_+$  and  $\mathcal{D}_-$  which we define to be the unique Choi-Jamiolkowski preimages of  $\hat{\omega}_{\text{A}'\text{E}}$ ,  $\Delta_+$  and  $\Delta_-$  respectively. Now we are in the position to apply the  $\varepsilon$ -almost decoupling theorem on  $\hat{\rho}$  and  $\hat{\omega}$  to find

$$\begin{aligned} & \sqrt{1 + 4\varepsilon d_{\text{A}}^4} 2^{-\frac{1}{2}} H_{\min}^\delta(\text{A}'|\text{E})_{\omega} - \frac{1}{2} H_{\min}^\delta(\text{A}|\text{R})_{\rho} \\ &= \sqrt{1 + 4\varepsilon d_{\text{A}}^4} 2^{-\frac{1}{2}} H_{\min}(\text{A}'|\text{E})_{\hat{\omega}} - \frac{1}{2} H_{\min}(\text{A}|\text{R})_{\hat{\rho}} \end{aligned} \quad (4.4)$$

$$\geq \sqrt{1 + 4\varepsilon d_{\text{A}}^4} 2^{-\frac{1}{2}} H_2(\text{A}'|\text{E})_{\hat{\omega}} - \frac{1}{2} H_2(\text{A}|\text{R})_{\hat{\rho}} \quad (4.5)$$

$$\geq \sum_i p_i \left\| \hat{\mathcal{T}}((U_{\text{A}}^i \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}} ((U_{\text{A}}^i)^\dagger \otimes \mathbb{1}_{\text{R}})) - \hat{\omega}_{\text{E}} \otimes \hat{\rho}_{\text{R}} \right\|_1. \quad (4.6)$$

To obtain a smoothed version of the  $\varepsilon$ -almost decoupling formula we need to get rid of the hat-terms in the above expression using  $\delta$ -bounds only. This is realized with several applications of the triangle inequality. For any  $i$ , we have

$$\begin{aligned} & \left\| \hat{\mathcal{T}}((U_{\text{A}}^i \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}} ((U_{\text{A}}^i)^\dagger \otimes \mathbb{1}_{\text{R}})) - \hat{\omega}_{\text{E}} \otimes \hat{\rho}_{\text{R}} \right\|_1 \\ & \geq \left\| \hat{\mathcal{T}}((U_{\text{A}}^i \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}} ((U_{\text{A}}^i)^\dagger \otimes \mathbb{1}_{\text{R}})) - \omega_{\text{E}} \otimes \hat{\rho}_{\text{R}} \right\|_1 - \|\omega_{\text{A}'\text{E}} - \hat{\omega}_{\text{A}'\text{E}}\|_1 \end{aligned} \quad (4.7)$$

$$\geq \left\| \hat{\mathcal{T}}((U_{\text{A}}^i \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}} ((U_{\text{A}}^i)^\dagger \otimes \mathbb{1}_{\text{R}})) - \omega_{\text{E}} \otimes \hat{\rho}_{\text{R}} \right\|_1 - 2\delta. \quad (4.8)$$

In the same way  $\hat{\rho}_{\text{R}}$  is eliminated from the product term and we get in total

$$\begin{aligned} & \left\| \hat{\mathcal{T}}((U_{\text{A}}^i \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}} ((U_{\text{A}}^i)^\dagger \otimes \mathbb{1}_{\text{R}})) - \hat{\omega}_{\text{E}} \otimes \hat{\rho}_{\text{R}} \right\|_1 \\ & \geq \left\| \hat{\mathcal{T}}((U_{\text{A}}^i \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}} ((U_{\text{A}}^i)^\dagger \otimes \mathbb{1}_{\text{R}})) - \omega_{\text{E}} \otimes \rho_{\text{R}} \right\|_1 - 4\delta. \end{aligned} \quad (4.9)$$



Still  $\hat{\mathcal{T}}$  and  $\hat{\rho}_{\text{AR}}$  occur in the above expression. To recover the original expression, over which the summation takes place, we need to rewrite the above using  $\mathcal{T}$  and  $\rho_{\text{AR}}$  only. This is achieved with two further applications of the triangle inequality.

$$\begin{aligned}
& \left\| \hat{\mathcal{T}}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \omega_{\text{E}} \otimes \rho_{\text{R}} \right\|_1 - 4\delta \\
& \geq \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \omega_{\text{E}} \otimes \rho_{\text{R}} \right\|_1 \\
& \quad - \left\| \hat{\mathcal{T}}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 - 4\delta
\end{aligned} \tag{4.10}$$

$$\begin{aligned}
& \geq \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \rho_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \omega_{\text{E}} \otimes \rho_{\text{R}} \right\|_1 \\
& \quad - \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \rho_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 \\
& \quad - \left\| \hat{\mathcal{T}}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 - 4\delta
\end{aligned} \tag{4.11}$$

The first term of equation (4.11) corresponds to the unsmoothed decoupling formula. For the remaining two terms

$$\sum_i p_i \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \rho_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 \tag{4.12}$$

and

$$\sum_i p_i \left\| \hat{\mathcal{T}}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 \tag{4.13}$$

we need to find upper bounds. We treat them separately beginning with the first one. To preform the calculation we write  $\hat{\rho} - \rho = \Gamma_+ - \Gamma_-$  and use the linearity of  $\mathcal{T}$ . We

get

$$\sum_i p_i \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \rho_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 \quad (4.14)$$

$$= \sum_i p_i \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \Gamma_+((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \Gamma_-((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 \quad (4.15)$$

$$\leq \sum_{a \in \{+, -\}} \sum_i p_i \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \Gamma_a((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 \quad (4.16)$$

$$= \sum_{a \in \{+, -\}} \text{tr} \left( \mathcal{T} \left( \sum_i p_i U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}} \Gamma_a (U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} - \int_{\text{U}} U_{\text{A}} \otimes \mathbb{1}_{\text{R}} \Gamma_a U^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} dU \right) \right) \\ + \sum_{a \in \{+, -\}} \text{tr} \left( \mathcal{T} \left( \int_{\text{U}} U_{\text{A}} \otimes \mathbb{1}_{\text{R}} \Gamma_a U^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} dU \right) \right) \quad (4.17)$$

$$\leq \sum_{a \in \{+, -\}} \left\| \sum_i p_i U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}} \Gamma_a (U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} - \int_{\text{U}} U_{\text{A}} \otimes \mathbb{1}_{\text{R}} \Gamma_a U^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} dU \right\|_1 \left\| \mathcal{T}^\dagger(\mathbb{1}_{\text{E}}) \right\|_\infty \\ + \sum_{a \in \{+, -\}} \text{tr}(\mathcal{T}(\pi_{\text{A}}) \otimes \text{tr}_{\text{A}} \Gamma_a) \quad (4.18)$$

$$\leq \sum_{a \in \{+, -\}} \varepsilon \left\| \Gamma_a \right\|_1 \left\| \mathcal{T}^\dagger(\mathbb{1}_{\text{E}}) \right\|_\infty + \sum_{a \in \{+, -\}} \text{tr}(\omega_{\text{A}'\text{E}}) \text{tr}(\Gamma_a). \quad (4.19)$$

In the last inequality we used the property of the almost 2-design that it constitutes an almost 1-design automatically. This can be seen straight from the definition considering states that are given by the identity operator on one of the systems on which the unitaries act. Now choose the eigenvalue of  $\mathcal{T}^\dagger(\mathbb{1}_{\text{E}})$  which is biggest in absolute value. Let  $P_{\text{A}}$  be the projector corresponding to this eigenvalue. Note, moreover, that  $\text{tr}(\Gamma_a) \leq 2\delta$  as we have already shown. Using all this, we get

$$\sum_i p_i \left\| \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \rho_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 \\ \leq 4\varepsilon \delta \left\| \mathcal{T}^\dagger(\mathbb{1}_{\text{E}}) \right\|_\infty + 4\delta \quad (4.20)$$

$$\leq 4\varepsilon \delta \text{tr}(\mathcal{T}(P_{\text{A}})) + 4\delta \quad (4.21)$$

$$= 4d_{\text{A}}\varepsilon\delta \text{tr}(\omega_{\text{A}'\text{E}}(P_{\text{A}})^\dagger \otimes \mathbb{1}_{\text{E}}) + 4\delta \quad (4.22)$$

$$\leq 4d_{\text{A}}\varepsilon\delta \text{tr}(\omega_{\text{A}'\text{E}}) \left\| (P_{\text{A}})^\dagger \otimes \mathbb{1}_{\text{E}} \right\|_\infty + 4\delta \quad (4.23)$$

$$\leq 4d_{\text{A}}\varepsilon\delta + 4\delta. \quad (4.24)$$

The last step makes use of the fact that  $(P_{\text{A}})^\dagger$  being a projector has positive eigenvalues smaller or equal than one. For the evaluation of the second term (4.13) we decompose  $\hat{\mathcal{T}} - \mathcal{T} = \mathcal{D}_+ - \mathcal{D}_-$  in accordance with the above decomposition  $\hat{\omega} - \omega = \Delta_+ - \Delta_-$ .

We then get

$$\begin{aligned} & \sum_i p_i \left\| \hat{\mathcal{T}}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) - \mathcal{T}((U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}}((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}})) \right\|_1 \\ &= \sum_i p_i \left\| (\mathcal{D}_+ - \mathcal{D}_-) (U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}} \hat{\rho}_{\text{AR}} (U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \right\|_1 \end{aligned} \quad (4.25)$$

$$\leq \sum_{a \in \{+, -\}} \sum_i p_i \left\| \mathcal{D}_a (U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}} \hat{\rho}_{\text{AR}} (U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \right\|_1 \quad (4.26)$$

$$\leq \sum_{a \in \{+, -\}} \text{tr} \left( \mathcal{D}_a \left( \sum_i p_i (U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \hat{\rho}_{\text{AR}} ((U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}}) \right) \right) \quad (4.27)$$

$$\begin{aligned} &= \sum_{a \in \{+, -\}} \text{tr} \left( \mathcal{D}_a \left( \sum_i p_i U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}} \hat{\rho}_{\text{AR}} (U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} - \int_{\mathbb{U}} U_{\text{A}} \otimes \mathbb{1}_{\text{R}} \hat{\rho}_{\text{AR}} U^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} dU \right) \right) \\ &+ \sum_{a \in \{+, -\}} \text{tr} \left( \mathcal{D}_a \left( \int_{\mathbb{U}} U_{\text{A}} \otimes \mathbb{1}_{\text{R}} \hat{\rho}_{\text{AR}} U^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} dU \right) \right) \end{aligned} \quad (4.28)$$

$$\begin{aligned} &\leq \sum_{a \in \{+, -\}} \left\| \sum_i p_i U^i_{\text{A}} \otimes \mathbb{1}_{\text{R}} \hat{\rho}_{\text{AR}} (U^i)^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} - \int_{\mathbb{U}} U_{\text{A}} \otimes \mathbb{1}_{\text{R}} \hat{\rho}_{\text{AR}} U^\dagger_{\text{A}} \otimes \mathbb{1}_{\text{R}} dU \right\|_1 \left\| \mathcal{D}_a^\dagger(\mathbb{1}_{\text{E}}) \right\|_\infty \\ &+ \sum_{a \in \{+, -\}} \text{tr} (\mathcal{D}_a(\pi_{\text{A}} \otimes \hat{\rho}_{\text{R}})) \end{aligned} \quad (4.29)$$

$$\leq \sum_{a \in \{+, -\}} \varepsilon \left\| \hat{\rho}_{\text{AR}} \right\|_1 \left\| \mathcal{D}_a^\dagger(\mathbb{1}_{\text{E}}) \right\|_\infty + \sum_{a \in \{+, -\}} \text{tr} (\Delta_a \otimes \hat{\rho}_{\text{R}}). \quad (4.30)$$

Again, we used the fact that an almost 2-design (4.30) is an almost 1-design automatically. Thus we can use the bound with the diamond norm here, too. Furthermore, note that  $\hat{\rho}_{\text{AR}}$  is sub-normalized by definition and that we found that  $\|\Delta_a\|_1 \leq 2\delta$ . We define  $P_{\text{A}}^a$  to be the projector corresponding to the biggest absolute eigenvalue of

$\mathcal{D}_a^\dagger(\mathbf{1}_E)$  and we get that

$$\begin{aligned} & \sum_i p_i \left\| \hat{\mathcal{T}}((U^i_A \otimes \mathbf{1}_R) \hat{\rho}_{AR}((U^i_A)^\dagger \otimes \mathbf{1}_R)) - \mathcal{T}((U^i_A \otimes \mathbf{1}_R) \hat{\rho}_{AR}((U^i_A)^\dagger \otimes \mathbf{1}_R)) \right\|_1 \\ & \leq \sum_{a \in \{+, -\}} \varepsilon \left\| \mathcal{D}_a^\dagger(\mathbf{1}_E) \right\|_\infty + 4\delta \end{aligned} \quad (4.31)$$

$$= \sum_{a \in \{+, -\}} \varepsilon \operatorname{tr} (P_A^a \mathcal{D}_a^\dagger(\mathbf{1}_E)) + 4\delta \quad (4.32)$$

$$= \sum_{a \in \{+, -\}} \varepsilon \operatorname{tr} (\mathcal{D}_a(P_A^a)) + 4\delta \quad (4.33)$$

$$= d_A \sum_{a \in \{+, -\}} \varepsilon \operatorname{tr} (\Delta_a ((P_A^a)^\top \otimes \mathbf{1}_E)) + 4\delta \quad (4.34)$$

$$\leq d_A \sum_{a \in \{+, -\}} \varepsilon \|\Delta_a\|_1 \|(P_A^a)^\top \otimes \mathbf{1}_E\|_\infty + 4\delta \quad (4.35)$$

$$= 4d_A \varepsilon \delta + 4\delta. \quad (4.36)$$

In the last step we used the fact that the biggest eigenvalue of  $(P_A^a)^\top$  is one.

Taking together the expressions (4.24) and (4.36) and plugging them into (4.11), we obtain

$$\begin{aligned} & \sum_i p_i \left\| \hat{\mathcal{T}}((U^i_A \otimes \mathbf{1}_R) \hat{\rho}_{AR}((U^i_A)^\dagger \otimes \mathbf{1}_R)) - \hat{\omega}_E \otimes \hat{\rho}_R \right\|_1 \\ & \geq \sum_i p_i \left\| \mathcal{T}((U^i_A \otimes \mathbf{1}_R) \rho_{AR}((U^i_A)^\dagger \otimes \mathbf{1}_R)) - \omega_E \otimes \rho_R \right\|_1 - 4d_A \varepsilon \delta - 4\delta - 4d_A \varepsilon \delta - 4\delta - 4\delta. \end{aligned} \quad (4.37)$$

Finally this yields

$$\begin{aligned} & \sum_i p_i \left\| \mathcal{T}((U^i_A \otimes \mathbf{1}_R) \rho_{AR}((U^i_A)^\dagger \otimes \mathbf{1}_R)) - \omega_E \otimes \rho_R \right\|_1 \\ & \leq \sqrt{1 + 4\varepsilon d_A^4} 2^{-\frac{1}{2} H_{\min}^\delta(A|E)_\omega - \frac{1}{2} H_{\min}^\delta(A|R)_\rho} + 8d_A \varepsilon \delta + 12\delta, \end{aligned} \quad (4.38)$$

which proves the smoothed decoupling formula for  $\varepsilon$ -approximate 2-designs.

## Chapter 5

# A classical analogue of the decoupling formula

The decoupling theorem bounds the average distance of some quantum state after a random unitary operation and some quantum channel have been applied to it from a fully uncorrelated state. Generally a unitary operation on a quantum system  $A$  corresponds to a quantum-mechanical evolution of this system. Thus the decoupling theorem is only relevant under the assumption that the evolution is governed by the laws of quantum mechanics. In this and the following chapters we would like to understand in how far classical operations can be used for decoupling purposes. Instead of averaging over the group of all unitary matrices  $\mathbb{U}(A)$ , we restrict the problem to the case where only classical operations are allowed, i. e. we average over the group of all permutation operators on the system  $A$ ,  $\mathbb{P}(A)$ . This corresponds physically to a situation where a system is subject to an evolution which is purely classical. Or, from the point of view of the computational sciences, we restrict our analysis to operations that can be performed on a classical computer in contrast to a quantum computer. While it turns out that this problem is difficult to solve in the general case, several special cases of particular interest will be studied in the sequel. In this chapter we assume that the state of the  $A$  system is classical, but still we allow that it has correlations with a reference quantum-system  $R$ . A typical situation, where this is the case is that the  $A$  system represents the outcome of a random variable and an adversary possesses quantum side information about  $A$ . The question we are interested in is whether using some classical operation it is possible to extract from  $A$  a part that is almost completely unknown to the adversary. Our discussion will give results strongly resembling the “General Leftover Hash Lemma” as derived in [15], which has large-scale implications in the area of quantum cryptography.

## 5.1 A “classicalized” Decoupling Lemma

The aim of this section is to derive a decoupling lemma as in Section 2.1 for our new setup, where the integration over the unitary group is replaced by an average over all permutation operators and the quantum state under consideration has CQ-structure. For completeness we shortly recover some terminology and basic definitions:

The *symmetric group*  $S_n$  is the set of all bijections of  $\{1, \dots, n\}$  to itself together with the concatenation of maps as the group multiplication. Elements  $\pi$  of  $S_n$  are called *permutations*.

**Definition 9.** (Permutation operator [18]) Let  $\mathcal{H}_A$  be a Hilbert space together with a fixed basis  $\{|i\rangle\}_{i=1, \dots, d_A}$ . For  $\pi$  in  $S_{d_A}$ , we define the permutation operator  $P(\pi)$  to be the operator which has the matrix representation  $(P_{ij})$ , where

$$(P_{ij}) = \begin{cases} 1 & \text{if } \pi(j) = i \\ 0 & \text{otherwise} \end{cases}$$

with respect to the given basis.

For a given Hilbert space  $\mathcal{H}_A$ , we denote by  $\mathbb{P}(A)$  the set of all permutation operators for some fixed basis. This set has  $d_A!$  elements. Since the above definition includes a group homomorphism from  $S_{d_A}$  to the group of automorphisms of  $\mathcal{H}_A$ , it defines a representation ([18]) of the symmetric group  $S_{d_A}$  called the *defining representation*.

Furthermore we define what is meant by a CQ-state.

**Definition 10.** (CQ-state [16]) Let  $\mathcal{H}_A$  and  $\mathcal{H}_R$  be Hilbert spaces and let  $\{|i\rangle\}_{i=1, \dots, d_A}$  be a fixed orthonormal basis of  $\mathcal{H}_A$ . A density operator  $\rho_{AR} \in \mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_R)$  is said to be classical on  $\mathcal{H}_A$  with respect to the basis  $\{|i\rangle\}_{i=1, \dots, d_A}$  if

$$\rho_{AR} \in \text{span}\{|i\rangle\langle i|_{i=1, \dots, d_A}\} \otimes \mathcal{L}^{\dagger}(\mathcal{H}_R).$$

If in addition  $\rho_{AR}$  is non-classical on  $\mathcal{H}_R$ , we call it a hybrid classical-quantum state or shortly CQ-state.

Typically CQ-states are used in situations, where the quantum state of some system (here  $R$ ) is not known with certainty. Instead it depends on the outcome of some classical random event (described by system  $A$  in our case). Note that a

CQ-state  $\rho_{AR}$  can be written in the basis  $\{|i\rangle\}_{i=1,\dots,d_A}$  introduced in the definition to be

$$\rho_{AR} = \sum_i |i\rangle\langle i|_A \otimes \rho_R^{[i]}, \quad (5.1)$$

where the  $\rho_R^{[i]}$  are sub-normalized density operators with  $\sum_i \rho_R^{[i]} = \rho_R$ .

Finally for a linear map  $\mathcal{T}_{A \rightarrow E} \in \text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$ , we define its classicalized version  $\mathcal{T}_{A \rightarrow E}^{cl}$ .

**Definition 11.** (Classicalized map) Let  $\mathcal{H}_A$  be a Hilbert space with a fixed orthonormal basis  $\{|i\rangle\}_{i=1,\dots,d_A}$  and let  $\mathcal{T}_{A \rightarrow E}$  be a linear map in  $\text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$ . We define the map  $\mathcal{T}_{A \rightarrow E}^{cl} \in \text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$  by

$$\mathcal{T}_{A \rightarrow E}^{cl}(\rho_A) := \mathcal{T}_{A \rightarrow E} \left( \sum_i |i\rangle\langle i|_A \rho_A |i\rangle\langle i|_A \right) \quad \forall \rho_A \in \mathcal{L}(\mathcal{H}_A)$$

and call  $\mathcal{T}_{A \rightarrow E}^{cl}$  the classicalized version of  $\mathcal{T}_{A \rightarrow E}$ .

The Choi-Jamiołkowski representation of  $\mathcal{T}_{A \rightarrow E}^{cl}$  will be denoted by  $\omega_{A'E}^{cl}$ , i. e.

$$\omega_{A'E}^{cl} = \mathcal{T}_{A \rightarrow E}^{cl}(\Phi_{AA'}) \quad (5.2)$$

$$= \mathcal{T}_{A \rightarrow E} \left( \sum_i |i\rangle\langle i|_A \Phi_{AA'} |i\rangle\langle i|_A \right) \quad (5.3)$$

$$= \mathcal{T}_{A \rightarrow E} \left( \frac{1}{d_A} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_{A'} \right) \quad (5.4)$$

$$=: \mathcal{T}_{A \rightarrow E}(T_{AA'}), \quad (5.5)$$

where in the last equation we introduced the state  $T_{AA'} := \frac{1}{d_A} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_{A'}$ , which includes the classical correlations between the systems  $A$  and  $A'$ . From equation (5.4) one can see that the Choi-Jamiołkowski representation of a classicalized map always has CQ-structure. A short calculation reveals that

$$\omega_E = \omega_E^{cl}. \quad (5.6)$$

The term “classicalized map” is motivated by the fact that applying such a map to a state  $\rho_{AR}$  always produces a CQ-state. Moreover it does not matter whether one applies a map  $\mathcal{T}_{A \rightarrow E}$  or its classicalized version  $\mathcal{T}_{A \rightarrow E}^{cl}$  on a CQ-state. We get assuming that  $\rho_{AR}$  has CQ-structure that

$$\mathcal{T}_{A \rightarrow E}^{cl}(\rho_{AR}) = \mathcal{T}_{A \rightarrow E} \left( \sum_j |j\rangle\langle j|_A \left( \sum_i |i\rangle\langle i|_A \otimes \rho_R^{[i]} \right) |j\rangle\langle j|_A \right) \quad (5.7)$$

$$= \mathcal{T}_{A \rightarrow E}(\rho_{AR}). \quad (5.8)$$

In fact this is intuitively clear. The state  $\rho_{AR}$  is already classical on  $A$ ; further classicalization of this state has no effect anymore. We are now in the position to state the decoupling lemma for CQ-states.

**Lemma:** (Decoupling Lemma for CQ-states) *Let  $\rho_{AR}$  be classical on  $\mathcal{H}_A$  with respect to  $\{|i\rangle\}_{i=1,\dots,d_A}$  and let  $\mathcal{T}_{A \rightarrow E} \in \text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$  be a linear map with Choi-Jamiołkowski representation  $\omega_{A'E} \in \mathcal{L}^\dagger(\mathcal{H}_E \otimes \mathcal{H}_{A'})$ , then*

$$\begin{aligned} \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_2^2 \\ = \frac{d_A^2}{d_A - 1} \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_2^2 \left\| \omega_{A'E}^{cl} - \pi_{A'} \otimes \omega_E^{cl} \right\|_2^2, \end{aligned}$$

where the summation goes over all permutation operators, which act by permuting the basis vectors of  $\{|i\rangle\}_{i=1,\dots,d_A}$ .

Since conjugating  $\rho_{AR}$  with a permutation operator acting on  $A$  does not affect its CQ-structure, one can apply equation (5.8) directly to the statement of the decoupling lemma for CQ-states. Together with equation (5.6) this results in

$$\begin{aligned} \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_2^2 \\ = \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}^{cl}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E^{cl} \otimes \rho_R \right\|_2^2, \end{aligned} \quad (5.9)$$

which explains the occurrence of the Choi-Jamiołkowski representation of  $\mathcal{T}_{A \rightarrow E}^{cl}$  on the right hand side of the lemma.

The rest of this section is devoted to a proof of the Decoupling Lemma for CQ-states. This proof will be organized in three subsections. In the first and second we proof two general claims about the action of permutation operators and apply them in the third subsection to conclude the proof.

### 5.1.1 Counting permutation operators

The following claim will be useful in our proof. It shows how twofold tensor products of permutation operators act on classical states.



**Claim 1:** Let  $\{|i\rangle\}_{i=1,\dots,d_A}$  with  $d_A \geq 2$  be some basis and  $\mathbb{P}(A)$  be the corresponding set of permutation operators. Then for any  $i, j$

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes P_{A'}) (|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (P_A^\dagger \otimes P_{A'}^\dagger) = \frac{1 - \delta_{ij}}{d_A^2 - d_A} \mathbb{1}_{AA'} - \frac{1 - \delta_{ij}}{d_A - 1} T_{AA'} + \delta_{ij} T_{AA'}.$$

This formula can be seen as follows. Consider first the case when  $i = j$  then

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes P_{A'}) (|i\rangle\langle i|_A \otimes |i\rangle\langle i|_{A'}) (P_A^\dagger \otimes P_{A'}^\dagger) = \frac{(d_A - 1)!}{d_A!} \sum_k |k\rangle\langle k|_A \otimes |k\rangle\langle k|_{A'}, \quad (5.10)$$

$$= T_{AA'}, \quad (5.11)$$

The crucial step in equation (5.10) can be seen from an easy counting argument. Since the permutations are bijective maps for any  $|j\rangle, |k\rangle \in \{|i\rangle\}_{i=1,\dots,d_A}$  there are  $(d_A - 1)!$  permutation operators with  $P|j\rangle = |k\rangle$ . Thus when summing over all permutation operators as in equation (5.10) for any fixed  $|i\rangle$  every basis vector in  $\{|i\rangle\}_{i=1,\dots,d_A}$  contributes  $(d_A - 1)!$  times to the whole sum. The above implies that Claim 1 is valid for  $i = j$ . Now assume that  $i \neq j$ . For fixed  $k \neq l$  there are  $(d_A - 2)!$  permutation operators that map  $|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}$  to  $|k\rangle\langle k|_A \otimes |l\rangle\langle l|_{A'}$ , but there is no permutation operator mapping  $|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}$  to  $|k\rangle\langle k|_A \otimes |l\rangle\langle l|_{A'}$  with  $k = l$ . We conclude that in the case  $i \neq j$  we have

$$\begin{aligned} & \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes P_{A'}) (|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (P_A^\dagger \otimes P_{A'}^\dagger) \\ &= \frac{(d_A - 2)!}{d_A!} \sum_{k \neq l} |k\rangle\langle k|_A \otimes |l\rangle\langle l|_{A'}, \end{aligned} \quad (5.12)$$

$$= \frac{1}{d_A(d_A - 1)} \sum_{k,l} |k\rangle\langle k|_A \otimes |l\rangle\langle l|_{A'} - \frac{1}{d_A(d_A - 1)} \sum_k |k\rangle\langle k|_A \otimes |k\rangle\langle k|_{A'}, \quad (5.13)$$

$$= \frac{1}{d_A(d_A - 1)} \mathbb{1}_{AA'} - \frac{1}{d_A - 1} T_{AA'}. \quad (5.14)$$

So Claim 1 is also valid in the case that  $i \neq j$ , which concludes the proof. Finally we note that Claim 1 is intuitively clear: If we choose a permutation operator uniformly at random from  $\mathbb{P}$  and apply  $P \otimes P$  to any state of the type  $|i\rangle \otimes |i\rangle$  we expect to get the uniform distribution over the set of such states. Since there are  $d_A$  such states, the result of the summation should be  $T$  for  $i = j$ . If  $i \neq j$  we still expect that applying  $P \otimes P$  to  $|i\rangle \otimes |j\rangle$  yields the uniform distribution on the set of  $|i\rangle \otimes |j\rangle$ . Since there are  $d_A(d_A - 1)$  such states, the result of the summation in this case is

$$\frac{1}{d_A(d_A - 1)} \sum_{k \neq l} |k\rangle\langle k| \otimes |l\rangle\langle l|. \quad (5.15)$$

### 5.1.2 Action of twofold tensor products of permutation operators on a CQ-decoupling state.

In the next subsection we will see that in order to proof the CQ-Decoupling Lemma one can proceed similarly as was done in the proof of the usual Decoupling Lemma with unitary operations in Section 2.1. There it was convenient to introduce the Decoupling State  $\xi_{A\bar{A}} := \Phi_{A\bar{A}} - \pi_A \otimes \pi_{\bar{A}}$ . Here a similar approach will be used but this time we work with the CQ-Decoupling State  $\lambda_{A\bar{A}} := T_{A\bar{A}} - \pi_A \otimes \pi_{\bar{A}}$ . This subsection shows a mathematical claim about that state. In the next subsection we will see why  $\lambda_{A\bar{A}}$  is of relevance and use our claim.

**Claim 2:** Let  $\lambda_{A\bar{A}} = T_{A\bar{A}} - \pi_A \otimes \pi_{\bar{A}}$  be the CQ-Decoupling State. In the setup of the previous section with  $d_A \geq 2$ , we have that

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} (\lambda_{A\bar{A}})^{\otimes 2} (P_A^\dagger \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} = \frac{1}{d_A - 1} (\lambda_{A\bar{A}'} \otimes \lambda_{\bar{A}\bar{A}'}).$$

A conceptually easy way of proving this is by writing out  $\lambda_{A\bar{A}} = T_{A\bar{A}} - \pi_A \otimes \pi_{\bar{A}}$ , which gives

$$\begin{aligned} \lambda_{A\bar{A}}^{\otimes 2} &= T_{A\bar{A}} \otimes T_{A'\bar{A}'} \\ &\quad - T_{A\bar{A}} \otimes \pi_{A'\bar{A}'} \\ &\quad - \pi_{A\bar{A}} \otimes T_{A'\bar{A}'} \\ &\quad + \pi_{A\bar{A}} \otimes \pi_{A'\bar{A}'} \end{aligned} \tag{5.16}$$

and by applying the summation to the four different terms separately. The last term is invariant under the summation. For the second term we get

$$\begin{aligned} &\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} (T_{A\bar{A}} \otimes \pi_{A'\bar{A}'})(P_A^\dagger \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} \\ &= \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes \mathbb{1}_{\bar{A}}) T_{A\bar{A}} (P_A^\dagger \otimes \mathbb{1}_{\bar{A}}) \otimes \pi_{A'\bar{A}'}, \end{aligned} \tag{5.17}$$

$$= \frac{1}{d_A d_A!} \sum_i \sum_{P_A \in \mathbb{P}(A)} (P_A |i\rangle\langle i|_A P_A^\dagger) \otimes |i\rangle\langle i|_{\bar{A}} \otimes \pi_{A'\bar{A}'}, \tag{5.18}$$

$$= \frac{(d_A - 1)!}{d_A d_A!} \sum_i \mathbb{1}_A \otimes |i\rangle\langle i|_{\bar{A}} \otimes \pi_{A'\bar{A}'}, \tag{5.19}$$

$$= \pi_{A\bar{A}} \otimes \pi_{A'\bar{A}'}. \tag{5.20}$$

In (5.19) we again used the fact that for any  $|j\rangle, |k\rangle \in \{|i\rangle\}_{i=1, \dots, d_A}$  there are  $(d_A - 1)!$  permutation operators with  $P|j\rangle = |k\rangle$ . Therefore in the sum over all permutation

operators in equation (5.19) for any fixed  $|i\rangle$  every basis vector in  $\{|i\rangle\}_{i=1,\dots,d_A}$  contributes  $(d_A - 1)!$  times to the whole sum.

Due to the symmetry of the problem the third and the second term in equation (5.16) yield the same result after summation, such that we only have to evaluate the sum over the first term.

$$\begin{aligned} & \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} (T_{A\bar{A}} \otimes T_{A'\bar{A}'}) (P_A^\dagger \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} \\ &= \frac{1}{d_A^2 d_A!} \sum_{i,j} \sum_{P_A \in \mathbb{P}(A)} (P_A |i\rangle\langle i|_A P_A^\dagger) \otimes |i\rangle\langle i|_{\bar{A}} \otimes (P_{A'} |j\rangle\langle j|_{A'} P_{A'}^\dagger) \otimes |j\rangle\langle j|_{\bar{A}'}, \end{aligned} \quad (5.21)$$

We now use Claim 1 and plug this result into equation (5.21).

$$\begin{aligned} & \frac{1}{d_A^2 d_A!} \sum_{i,j} \sum_{P_A \in \mathbb{P}(A)} (P_A |i\rangle\langle i|_A P_A^\dagger) \otimes |i\rangle\langle i|_{\bar{A}} \otimes (P_{A'} |j\rangle\langle j|_{A'} P_{A'}^\dagger) \otimes |j\rangle\langle j|_{\bar{A}'} \\ &= \frac{1}{d_A^2} \sum_{i,j} \left( \left( \frac{1 - \delta_{ij}}{d_A^2 - d_A} \mathbb{1}_{AA'} - \frac{1 - \delta_{ij}}{d_A - 1} T_{AA'} + \delta_{ij} T_{AA'} \right) \otimes |i\rangle\langle i|_{\bar{A}} \otimes |j\rangle\langle j|_{\bar{A}'} \right) \end{aligned} \quad (5.22)$$

$$\begin{aligned} &= \frac{1}{d_A^2} \sum_i (T_{AA'} \otimes |i\rangle\langle i|_{\bar{A}} \otimes |i\rangle\langle i|_{\bar{A}'}) \\ &+ \frac{1}{d_A^2} \sum_{i \neq j} \left( \left( \frac{1}{d_A^2 - d_A} \mathbb{1}_{AA'} - \frac{1}{d_A - 1} T_{AA'} \right) \otimes |i\rangle\langle i|_{\bar{A}} \otimes |j\rangle\langle j|_{\bar{A}'} \right) \end{aligned} \quad (5.23)$$

$$\begin{aligned} &= \frac{1}{d_A} T_{AA'} \otimes T_{\bar{A}\bar{A}'}, \\ &+ \frac{1}{d_A^2} \sum_{i,j} \left( \left( \frac{1}{d_A^2 - d_A} \mathbb{1}_{AA'} - \frac{1}{d_A - 1} T_{AA'} \right) \otimes |i\rangle\langle i|_{\bar{A}} \otimes |j\rangle\langle j|_{\bar{A}'} \right) \\ &- \frac{1}{d_A^2} \sum_i \left( \left( \frac{1}{d_A^2 - d_A} \mathbb{1}_{AA'} - \frac{1}{d_A - 1} T_{AA'} \right) \otimes |i\rangle\langle i|_{\bar{A}} \otimes |i\rangle\langle i|_{\bar{A}'} \right) \end{aligned} \quad (5.24)$$

$$\begin{aligned} &= \frac{1}{d_A} T_{AA'} \otimes T_{\bar{A}\bar{A}'}, \\ &+ \left( \frac{1}{d_A^2 - d_A} \mathbb{1}_{AA'} - \frac{1}{d_A - 1} T_{AA'} \right) \otimes \pi_{\bar{A}} \otimes \pi_{\bar{A}'}, \\ &- \frac{1}{d_A} \left( \frac{1}{d_A^2 - d_A} \mathbb{1}_{AA'} - \frac{1}{d_A - 1} T_{AA'} \right) \otimes T_{\bar{A}\bar{A}'}, \end{aligned} \quad (5.25)$$

$$= \frac{1}{d_A - 1} (\pi_{AA'} - T_{AA'}) \otimes (\pi_{\bar{A}\bar{A}'} - T_{\bar{A}\bar{A}'} + \pi_{AA'} \otimes \pi_{\bar{A}\bar{A}'}), \quad (5.26)$$

Taking this together with (5.20) and (5.16) yields that

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} (\lambda_{A\bar{A}})^{\otimes 2} (P_A^\dagger \otimes \mathbb{1}_{\bar{A}})^{\otimes 2} = \frac{1}{d_A - 1} (\pi_{AA'} - T_{AA'}) \otimes (\pi_{\bar{A}\bar{A}'} - T_{\bar{A}\bar{A}'}), \quad (5.27)$$

which concludes the proof of Claim 2.

### 5.1.3 Proof of the Decoupling Lemma for CQ-states

In this subsection we use Claim 2 to proof the Decoupling Lemma for CQ-states. For this we follow the discussion of Chapter 2.1. We introduce the map  $\mathcal{E}_{\tilde{A} \rightarrow R}^{cl}$ , which we define to be the unique Choi-Jamiołkowski preimage of the state  $\rho_{AR}$  i.e.  $\mathcal{E}_{\tilde{A} \rightarrow R}^{cl}(\Phi_{A\tilde{A}}) = \rho_{AR}$ , where  $\tilde{A}$  is just a copy of  $A$ . It suffices to consider classicalized maps  $\mathcal{E}_{\tilde{A} \rightarrow R}^{cl}$  because in our setup the state  $\rho_{AR}$  has CQ-structure. By our definition of a classicalized map, we conclude that there exists a map  $\mathcal{E}_{\tilde{A} \rightarrow R}$  with (compare (5.5))

$$\mathcal{E}(T_{A\tilde{A}}) = \rho_{AR}. \quad (5.28)$$

In addition we have that

$$\rho_R = \text{tr}_A(\mathcal{E}(T_{A\tilde{A}})) \quad (5.29)$$

$$= \mathcal{E}(\text{tr}_A(T_{A\tilde{A}})) \quad (5.30)$$

$$= \mathcal{E}(\pi_{\tilde{A}}). \quad (5.31)$$

Following the discussion of Chapter 2.1 equations (2.3), we can rewrite the term in the Schatten 2-norm for any permutation operator  $P_A$  as follows.

$$\begin{aligned} & \mathcal{T}((P_A \otimes \mathbb{1}_R) \rho_{AR} (P_A^\dagger \otimes \mathbb{1}_R)) - \omega_E \otimes \rho_R \\ &= \mathcal{T}((P_A \otimes \mathbb{1}_R) \mathcal{E}(T_{A\tilde{A}}) (P_A^\dagger \otimes \mathbb{1}_R)) - \mathcal{T}(\pi_A) \otimes \mathcal{E}(\pi_{\tilde{A}}) \end{aligned} \quad (5.32)$$

$$= (\mathcal{T} \otimes \mathcal{E})((P_A \otimes \mathbb{1}_{\tilde{A}})(T_{A\tilde{A}} - \pi_A \otimes \pi_{\tilde{A}})(P_A^\dagger \otimes \mathbb{1}_{\tilde{A}})) \quad (5.33)$$

$$= (\mathcal{T} \otimes \mathcal{E})((P_A \otimes \mathbb{1}_{\tilde{A}})(\lambda_{A\tilde{A}})(P_A^\dagger \otimes \mathbb{1}_{\tilde{A}})), \quad (5.34)$$

where in the last step we used the CQ-Decoupling State to simplify the notation. Then the left hand side of the CQ-Decoupling Lemma becomes

$$\begin{aligned} & \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_2^2 \\ &= \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \text{tr}((\mathcal{T} \otimes \mathcal{E})(P_A \otimes \mathbb{1}_{\tilde{A}} \lambda_{A\tilde{A}} P_A^\dagger \otimes \mathbb{1}_{\tilde{A}})^2) \end{aligned} \quad (5.35)$$

$$= \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \text{tr}(((P_A \otimes \mathbb{1}_{\tilde{A}})^{\otimes 2} (\lambda_{A\tilde{A}})^{\otimes 2} (P_A^\dagger \otimes \mathbb{1}_{\tilde{A}})^{\otimes 2}) (\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\mathcal{E}^\dagger)^{\otimes 2}[\mathcal{F}_R]) \quad (5.36)$$

$$= \text{tr} \left( \left( \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} (P_A \otimes \mathbb{1}_{\tilde{A}})^{\otimes 2} (\lambda_{A\tilde{A}})^{\otimes 2} (P_A^\dagger \otimes \mathbb{1}_{\tilde{A}})^{\otimes 2} \right) (\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \otimes (\mathcal{E}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right), \quad (5.37)$$

where equation (5.36) makes use of the swap trick (Appendix B) and is analogous to equation (2.11). We evaluate the sum over all permutation operators using Claim 2 which gives that

$$\begin{aligned} & \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_2^2 \\ &= \frac{1}{d_A - 1} \text{tr} \left( (\lambda_{AA'} \otimes \lambda_{\bar{A}\bar{A}'} ) (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \otimes (\mathcal{E}^\dagger)^{\otimes 2} [\mathcal{F}_R] \right) \end{aligned} \quad (5.38)$$

$$= \frac{1}{d_A - 1} \text{tr} \left( \mathcal{T}^{\otimes 2}(\lambda_{AA'}) \otimes \mathcal{E}^{\otimes 2}(\lambda_{\bar{A}\bar{A}'} ) \mathcal{F}_E \otimes \mathcal{F}_R \right) \quad (5.39)$$

$$= \frac{1}{d_A - 1} \text{tr} \left( \mathcal{T}^{\otimes 2}(\lambda_{AA'}) \mathcal{F}_E \right) \text{tr} \left( \mathcal{E}^{\otimes 2}(\lambda_{\bar{A}\bar{A}'} ) \mathcal{F}_R \right). \quad (5.40)$$

Due to the symmetry of the occurring trace terms it is sufficient to evaluate one of them. We get

$$\text{tr} \left( \mathcal{T}^{\otimes 2}(\lambda_{AA'}) \mathcal{F}_E \right) = \text{tr} \left( \mathcal{T}^{\otimes 2}(T_{AA'} - \pi_{AA'}) \mathcal{F}_E \right) \quad (5.41)$$

$$= \frac{1}{d_A} \sum_i \text{tr} \left( \mathcal{T}(|i\rangle\langle i|_A)^2 \right) - \text{tr}(\omega_E^2) \quad (5.42)$$

$$= \frac{1}{d_A} \sum_{i,j} \delta_{ij} \text{tr} \left( \mathcal{T}(|i\rangle\langle i|_A) \mathcal{T}(|j\rangle\langle j|_A) \right) - \text{tr}(\omega_E^2) \quad (5.43)$$

$$= \frac{1}{d_A} \sum_{i,j} \text{tr} \left( |i\rangle\langle i|_{A'} |j\rangle\langle j|_{A'} \otimes \mathcal{T}(|i\rangle\langle i|_A) \mathcal{T}(|j\rangle\langle j|_A) \right) - \text{tr}(\omega_E^2) \quad (5.44)$$

$$= \frac{1}{d_A} \text{tr} \left( \sum_i (|i\rangle\langle i|_{A'} \otimes \mathcal{T}(|i\rangle\langle i|_A)) \sum_j (|j\rangle\langle j|_{A'} \otimes \mathcal{T}(|j\rangle\langle j|_A)) \right) - \text{tr}(\omega_E^2) \quad (5.45)$$

$$= d_A \text{tr} \left( \mathcal{T}(T_{AA'}) \mathcal{T}(T_{AA'}) \right) - \text{tr}(\omega_E^2) \quad (5.46)$$

$$= d_A \left( \text{tr}((\omega_{A'E}^{cl})^2) - \frac{1}{d_A} \text{tr}(\omega_E^2) \right), \quad (5.47)$$

where the last step is by equation (5.5). An analogous calculation upon exploitation of the CQ-structure of  $\rho_{AR}$  yields that

$$\text{tr} \left( \mathcal{E}^{\otimes 2}(\lambda_{\bar{A}\bar{A}'} ) \mathcal{F}_R \right) = d_A \left( \text{tr}(\rho_{AR}^2) - \frac{1}{d_A} \text{tr}(\rho_R^2) \right). \quad (5.48)$$

We find plugging into equation (5.40) that

$$\begin{aligned} & \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_2^2 \\ &= \frac{d_A^2}{d_A - 1} \left( \text{tr}((\omega_{A'E}^{cl})^2) - \frac{1}{d_A} \text{tr}(\omega_E^2) \right) \left( \text{tr}(\rho_{AR}^2) - \frac{1}{d_A} \text{tr}(\rho_R^2) \right) \end{aligned} \quad (5.49)$$

$$= \frac{d_A^2}{d_A - 1} \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_2^2 \left\| \omega_{A'E}^{cl} - \pi_{A'} \otimes \omega_E^{cl} \right\|_2^2, \quad (5.50)$$

which concludes the proof of the Decoupling Lemma for CQ-states. In the next sections we derive three theorems from this lemma. The theorems get more general but partially we have to pay for this with worse bounds. The first one will be analogous to the “Leftover Hash Lemma” as derived in [15] while the second and third resemble the decoupling theorem.

## 5.2 A “Hash Lemma” like result

**Theorem:** (CQ-Decoupling Theorem for the Partial Trace) *Let  $\rho_{\text{AR}}$  be classical on  $\mathcal{H}_A$  with respect to  $\{|i\rangle\}_{i=1,\dots,d_A}$  and let  $A = (A_1 A_2)$  be a composite system, then the average distance from uniform is given by*

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \rho_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1 \leq \sqrt{d_{A_1} \frac{d_A - d_{A_2}}{d_A - 1} 2^{-H_{\min}(A|R)_\rho}},$$

where the average goes over all permutation operators, which act by permuting the basis vectors of  $\{|i\rangle\}_{i=1,\dots,d_A}$ .

This in particular implies that

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \rho_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1 \leq \sqrt{d_{A_1} 2^{-H_{\min}(A|R)_\rho}}. \quad (5.51)$$

In [15], [21] the “General Leftover Hash Lemma” is derived. There the summation takes place over all elements from some 2-universal family of hash functions from  $A$  to  $A_1$  [23] but the resulting bound is the same as in equation (5.51) i. e. slightly worse than in our theorem. Given a fixed state  $\rho_{\text{AR}}$  both the general leftover hash lemma and our theorem imply that there exists a function  $f : A \rightarrow A_1$  that extracts almost uniform randomness. We postpone a further analysis of this formula to the next chapter and for the moment turn our attention to the proof. We proceed as in Chapter 2.2 and apply the Hölder inequality (2.30) to bound the trace distance. Introducing the positive definite and normalized operator  $\zeta_R$ , we write:

$$\begin{aligned} & \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \rho_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1 \\ & \leq \left\| (\pi_{A_1} \otimes \zeta_R)^{-\frac{1}{4}} \left( \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \rho_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right) (\pi_{A_1} \otimes \zeta_R)^{-\frac{1}{4}} \right\|_2 \end{aligned} \quad (5.52)$$

$$= \sqrt{d_{A_1}} \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \tilde{\rho}_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \tilde{\rho}_R \right\|_2 \quad (5.53)$$

To keep the notation simple we introduced a state  $\tilde{\rho}_{\text{AR}} := (\mathbb{1}_{A_1} \otimes \zeta_R)^{-\frac{1}{4}} \rho_{\text{AR}} (\mathbb{1}_{A_1} \otimes \zeta_R)^{-\frac{1}{4}}$ . Applying equation (5.53) first and afterwards the decoupling lemma for CQ-states

(Section 5.1) yields

$$\begin{aligned} & \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1^2 \\ & \leq d_{A_1} \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \tilde{\rho}_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \tilde{\rho}_R \right\|_2^2 \end{aligned} \quad (5.54)$$

$$= d_{A_1} \frac{d_A^2}{d_A - 1} \left\| \tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R \right\|_2^2 \cdot \frac{1}{d_A} \cdot \left( 1 - \frac{1}{d_{A_1}} \right). \quad (5.55)$$

The last equation is an application of the CQ decoupling lemma, where we used the explicit form of the Choi-Jamiolkowski representation for the partial trace

$$\omega_{A'A_1}^{cl} = \text{tr}_{A_2}(T_{AA'}) \quad (5.56)$$

to calculate  $\left\| \omega_{A'E}^{cl} - \pi_{A'} \otimes \omega_E^{cl} \right\|_2^2$ . We conclude rewriting (5.55)

$$\begin{aligned} & \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1^2 \\ & \leq (d_{A_1} - 1) \frac{d_A}{d_A - 1} \left( \text{tr}(\tilde{\rho}_{AR}^2) - \frac{1}{d_A} \text{tr}(\tilde{\rho}_R^2) \right) \end{aligned} \quad (5.57)$$

$$\leq (d_{A_1} - 1) \frac{d_A}{d_A - 1} \text{tr}(\tilde{\rho}_{AR}^2) \quad (5.58)$$

$$= d_{A_1} \frac{d_A - d_{A_2}}{d_A - 1} \text{tr}(\tilde{\rho}_{AR}^2). \quad (5.59)$$

We choose now  $\zeta_R$  to minimize the above expression and use the fact that the  $H_{\min}$ -entropy always constitutes a lower bound on the  $H_2$ -entropy (*Lemma 5*) to arrive at

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1^2 \leq d_{A_1} \cdot \frac{d_A - d_{A_2}}{d_A - 1} \cdot 2^{-H_{\min}(A|R)_\rho}. \quad (5.60)$$

The proof is concluded by taking the square root on both sides and applying the Jensen inequality. It is also possible to follow the derivation of Section 2.3, where an “improved” decoupling theorem is derived to get bounds involving the  $H_{\min}$ -entropy and  $\sqrt{\left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_1}$ .

### 5.3 A decoupling theorem for CQ-states and TPCP maps

**Theorem:** (Decoupling Theorem for CQ-states and TPCP maps) *Let  $\rho_{AR} \in \mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_R)$  be classical on  $\mathcal{H}_A$  with respect to  $\{|i\rangle\}_{i=1, \dots, d_A}$  and let  $\mathcal{T}_{A \rightarrow E}$  be a completely*

positive and trace preserving, linear map then

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \|\mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R\|_1 \leq \sqrt{d_E \frac{d_A - \frac{d_A}{d_E}}{d_A - 1} 2^{-H_2(A|R)_\rho}},$$

where the average is taken over all permutation operators, which act by permuting the basis vectors of  $\{|i\rangle\}_{i=1,\dots,d_A}$ .

The proof is almost identical to the proof shown in the previous section. We apply the Hölder inequality as in (5.53) and the CQ-decoupling yields

$$\begin{aligned} & \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \|\mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R\|_1^2 \\ & \leq d_E \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \|\mathcal{T}(P_A \otimes \mathbb{1}_R \tilde{\rho}_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \tilde{\rho}_R\|_2^2 \end{aligned} \quad (5.61)$$

$$= d_E \frac{d_A^2}{d_A - 1} \|\tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R\|_2^2 \|\omega_{A'E}^{cl} - \pi_{A'} \otimes \omega_E^{cl}\|_2^2 \quad (5.62)$$

$$= d_E \frac{d_A^2}{d_A - 1} \|\tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R\|_2^2 \left( \text{tr}((\omega_{A'E}^{cl})^2) - \frac{1}{d_A} \text{tr}(\omega_E^2) \right) \quad (5.63)$$

$$= d_E \frac{1}{d_A - 1} \|\tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R\|_2^2 \left( \sum_i \text{tr}(\mathcal{T}(|i\rangle\langle i|_A)^2) - d_A \text{tr}(\omega_E^2) \right). \quad (5.64)$$

The last step makes use of the calculation following equation (5.42). By assumption  $\mathcal{T}$  is a TPCPM. Due to the trace preserving property, for any  $i$  we have  $\text{tr}(\mathcal{T}(|i\rangle\langle i|_A)) = 1$  and we know that all eigenvalues of  $\mathcal{T}(|i\rangle\langle i|_A)$  are nonnegative by the positivity of  $\mathcal{T}$ . We conclude that the eigenvalues of any matrix  $\mathcal{T}(|i\rangle\langle i|_A)$  are between zero and one. Thus

$$\text{tr}(\mathcal{T}(|i\rangle\langle i|_A)^2) \leq \text{tr}(\mathcal{T}(|i\rangle\langle i|_A)) \quad (5.65)$$

$$= 1. \quad (5.66)$$

Moreover an application of the Cauchy Schwarz inequality shows

$$1 = \text{tr}(\omega_E) \quad (5.67)$$

$$\leq \sqrt{\text{tr}(\mathbb{1}_E) \text{tr}(\omega_E^2)}. \quad (5.68)$$



Following (5.64) and using the found bounds we get that

$$\begin{aligned} & d_E \frac{1}{d_A - 1} \|\tilde{\rho}_{\text{AR}} - \pi_A \otimes \tilde{\rho}_{\text{R}}\|_2^2 \left( \sum_i \text{tr}(\mathcal{T}(|i\rangle\langle i|_A)^2) - d_A \text{tr}(\omega_{\text{E}}^2) \right) \\ & \leq d_E \frac{d_A - d_A \text{tr}(\omega_{\text{E}}^2)}{d_A - 1} \|\tilde{\rho}_{\text{AR}} - \pi_A \otimes \tilde{\rho}_{\text{R}}\|_2^2 \end{aligned} \quad (5.69)$$

$$\leq d_E \frac{d_A - \frac{d_A}{d_{\text{E}}}}{d_A - 1} \|\tilde{\rho}_{\text{AR}} - \pi_A \otimes \tilde{\rho}_{\text{R}}\|_2^2 \quad (5.70)$$

$$\leq d_E \frac{d_A - \frac{d_A}{d_{\text{E}}}}{d_A - 1} \text{tr}(\tilde{\rho}_{\text{AR}}^2). \quad (5.71)$$

The arguments following (5.59) conclude the proof.

## 5.4 A decoupling theorem for CQ-states

In this section a short derivation of a decoupling theorem for CQ-states is presented. The obtained theorem can be seen as a classical analogue of the decoupling theorem as derived in Section 2.2.

**Theorem:** (Decoupling Theorem for CQ-states) *Let  $\rho_{\text{AR}} \in \mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_{\text{R}})$  be classical on  $\mathcal{H}_A$  with respect to  $\{|i\rangle\}_{i=1,\dots,d_A}$  and let  $\mathcal{T}_{A \rightarrow \text{E}}$  be a completely positive linear map going from  $\mathcal{S}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_{\text{R}})$  to  $\mathcal{P}(\mathcal{H}_{\text{E}} \otimes \mathcal{H}_{\text{R}})$  with Choi-Jamiołkowski representation  $\omega_{\text{A}'\text{E}} \in \mathcal{S}_{\leq}(\mathcal{H}_{\text{E}} \otimes \mathcal{H}_{\text{A}'})$ , then*

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \|\mathcal{T}(P_A \otimes \mathbb{1}_{\text{R}} \rho_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_{\text{R}}) - \omega_{\text{E}} \otimes \rho_{\text{R}}\|_1 \leq \sqrt{(d_A + 1) 2^{-H_2(\text{A}|\text{R})_\rho - H_2(\text{A}'|\text{E})_{(\omega_{\text{cl}})}},$$

where the average is taken over all permutation operators, which act by permuting the basis vectors of  $\{|i\rangle\}_{i=1,\dots,d_A}$ .

The proof is closely analogous to the proof of the decoupling theorem as stated in Section 2.2. We therefore can keep our discussion short and refer to Section 2.2 for explanations. We apply the Hölder inequality as in (2.30) to get

$$\begin{aligned} & \|\mathcal{T}(P_A \otimes \mathbb{1}_{\text{R}} \rho_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_{\text{R}}) - \omega_{\text{E}} \otimes \rho_{\text{R}}\|_1 \\ & \leq \left\| (\sigma_{\text{E}} \otimes \zeta_{\text{R}})^{-\frac{1}{4}} \left( \mathcal{T}(P_A \otimes \mathbb{1}_{\text{R}} \rho_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_{\text{R}}) - \omega_{\text{E}} \otimes \rho_{\text{R}} \right) (\sigma_{\text{E}} \otimes \zeta_{\text{R}})^{-\frac{1}{4}} \right\|_2 \end{aligned} \quad (5.72)$$

$$= \left\| \tilde{\mathcal{T}}(P_A \otimes \mathbb{1}_{\text{R}} \tilde{\rho}_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_{\text{R}}) - \tilde{\omega}_{\text{E}} \otimes \tilde{\rho}_{\text{R}} \right\|_2, \quad (5.73)$$

where  $\sigma_E \in \mathcal{S}_=(\mathcal{H}_E)$  and  $\zeta_R \in \mathcal{S}_=(\mathcal{H}_R)$ . The map  $\tilde{\mathcal{T}}$  is defined as in Section 2.2 and  $\tilde{\omega}_{A'E}$  is the Choi-Jamiolkowski representation of  $\tilde{\mathcal{T}}$ . Furthermore we wrote  $\tilde{\rho}_{AR} := (\mathbb{1}_A \otimes \zeta_R)^{-\frac{1}{4}} \rho_{AR} (\mathbb{1}_A \otimes \zeta_R)^{-\frac{1}{4}}$ . Using the above inequality and applying the decoupling lemma for CQ-states yields

$$\begin{aligned} \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_1^2 \\ \leq \frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \tilde{\mathcal{T}}(P_A \otimes \mathbb{1}_R \tilde{\rho}_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \tilde{\omega}_E \otimes \tilde{\rho}_R \right\|_2^2 \end{aligned} \quad (5.74)$$

$$= \frac{d_A^2}{d_A - 1} \left\| \tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R \right\|_2^2 \left\| \tilde{\omega}_{A'E}^{cl} - \pi_{A'} \otimes \tilde{\omega}_E^{cl} \right\|_2^2 \quad (5.75)$$

$$= \frac{d_A^2}{d_A - 1} \left( \text{tr}(\tilde{\rho}_{AR}^2) - \frac{1}{d_A} \text{tr}(\tilde{\rho}_R^2) \right) \left( \text{tr}((\tilde{\omega}_{A'E}^{cl})^2) - \frac{1}{d_A} \text{tr}(\tilde{\omega}_E^{cl})^2 \right) \quad (5.76)$$

$$\leq (d_A + 1) \text{tr}((\tilde{\omega}_{A'E}^{cl})^2) \text{tr}(\tilde{\rho}_{AR}^2) \left( \frac{d_A^2 - \frac{d_A \text{tr}(\tilde{\omega}_E^{cl})^2}{\text{tr}((\tilde{\omega}_{A'E}^{cl})^2)}}{d_A^2 - 1} \right) \left( \frac{d_A^2 - \frac{d_A \text{tr}(\tilde{\rho}_R^2)}{\text{tr}(\tilde{\rho}_{AR}^2)}}{d_A^2 - 1} \right). \quad (5.77)$$

As discussed in Section 2.2 both bracket terms are smaller or equal than one and we get

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_1^2 \leq (d_A + 1) \text{tr}((\tilde{\omega}_{A'E}^{cl})^2) \text{tr}(\tilde{\rho}_{AR}^2). \quad (5.78)$$

We choose the  $\sigma_E$  and  $\zeta_R$  hidden in the tildes of the above expression to minimize the terms  $\text{tr}((\tilde{\omega}_{A'E}^{cl})^2)$  and  $\text{tr}(\tilde{\rho}_{AR}^2)$  to obtain a bound in terms of the  $H_2$ -entropy. Finally we take the square root on both sides and apply the Jensen inequality. This reveals that

$$\frac{1}{d_A!} \sum_{P_A \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_1 \leq \sqrt{(d_A + 1) 2^{-H_2(A|R)_\rho - H_2(A'|E)_{(\omega^{cl})}}}. \quad (5.79)$$

## Chapter 6

# Decoupling with 2-wise almost independent families of permutations

In the last chapter we dealt with an analogue of the decoupling theorem valid for CQ-states. It is now interesting to obtain a classical version of the results of Chapter 3. There the decoupling behavior of unitary almost 2-designs is discussed. But what is the classical analogue of a unitary almost 2-design? In this chapter's first section we introduce 2-wise almost independent families of permutations and show how they can be understood as a classical analogue of a unitary almost 2-design. Afterwards we generalize the versions of the decoupling theorem for CQ-states obtained in the previous chapter and formulate a result similar to the “General Leftover Hash Lemma” (*Lemma 2* in [21]). But instead of taking the average over a family of almost hash functions as is done in the latter, we average over almost independent permutations.

### 6.1 Almost independent families of permutations

The concept of  $k$ -wise independent permutations has been receiving an increasing amount of interest in the computer science literature (see [13] for an overview). Loosely speaking a family of permutations is called  $k$ -wise almost independent if for any element  $P$  chosen uniformly at random from that family and any  $k$  different input values  $x_1, \dots, x_k$  the distribution  $Px_1, \dots, Px_k$  is almost uniform. For our purposes it will be interesting to consider pairwise independent permutations, nevertheless we state the definitions for any  $k$  to emphasize the relation to unitary  $k$ -designs. In [12]

a construction of a family of  $k$ -wise almost independent permutations is given for any  $k$ .

**Definition 12.** (Statistical Distance [12]) Let  $D_1$  and  $D_2$  be two probability distributions defined over a finite set  $\Omega$ . The statistical distance of  $D_1$  and  $D_2$  is defined to be

$$\|D_1 - D_2\|_1 := \sum_{\omega \in \Omega} |D_1(\omega) - D_2(\omega)|$$

$D_1$  and  $D_2$  are called  $\varepsilon$ -close in statistical distance if  $\|D_1 - D_2\|_1 \leq \varepsilon$ .

Note that for two classical density operator  $\rho = \sum_i D_1(i)|i\rangle\langle i|$  and  $\sigma = \sum_i D_2(i)|i\rangle\langle i|$  the trace distance introduced in the preliminaries and the statistical distance of the corresponding distributions  $D_1$  and  $D_2$  coincide. Thus the trace distance can be viewed as a quantum generalization of the statistical distance, which justifies the above notation for the statistical distance with the “Schatten 1-norm”. If two probability distributions are  $\varepsilon$ -close in statistical distance the maximum difference between the probabilities of an arbitrary event with respect to the different distributions is smaller or equal than  $\varepsilon$ . We denote with  $\mathfrak{P}$  the family of all bijective functions

$$P : \{0, 1\}^n \rightarrow \{0, 1\}^n. \quad (6.1)$$

**Definition 13.** ( $k$ -wise  $\varepsilon$ -dependent family of permutations [12]) Let  $n, k \in \mathbb{N}$  and let  $[N_k]$  be the set of all  $k$ -tuples of *distinct*  $n$ -bit strings. Furthermore let  $\mathcal{F} \subset \mathfrak{P}$  be a family of permutations and  $\varepsilon \geq 0$ . The family  $\mathcal{F}$  is called  *$k$ -wise  $\varepsilon$ -dependent* if for every  $k$ -tuple  $(x_1, \dots, x_k) \in [N_k]$  and  $P$  chosen uniformly at random from  $\mathcal{F}$ , the distribution on  $[N_k]$  induced via  $(Px_1, \dots, Px_k)$  is  $\varepsilon$ -close to the uniform distribution on  $[N_k]$ . A  $k$ -wise 0-dependent family of permutations is called  *$k$ -wise independent*.

As already mentioned, in our setup pairwise almost independent permutations will be most relevant; similarly to the fact that we dealt with unitary almost 2-designs in Chapter 3. To reveal the relation between the definitions of almost independent permutations and unitary almost 2-designs (Definition 8) it is convenient to reformulate the above Definition 13 in terms of density operators. For this we first introduce some new notation. In analogy to Definition 6 we have:

**Definition 14.** For  $\mathcal{F} \subset \mathbb{P}$  and any  $\rho \in \mathcal{L}(\mathcal{H}^{\otimes k})$  we define the functions:

$$\begin{aligned} \mathcal{P}_W(\rho) &:= \sum_{P \in \mathcal{F}} \frac{1}{|\mathcal{F}|} P^{\otimes k} \rho (P^\dagger)^{\otimes k} \\ \mathcal{P}_H(\rho) &:= \sum_{P \in \mathbb{P}} \frac{1}{|\mathbb{P}|} P^{\otimes k} \rho (P^\dagger)^{\otimes k}. \end{aligned}$$

Note that in the above definition  $\mathcal{F}$  is a subset of  $\mathbb{P}$  and not of  $\mathfrak{P}$  as in Definition 13. We will see after some further definitions how this can be understood. To compare the distance of two maps we introduce a classical version of the diamond norm:

**Definition 15.** Fix an orthonormal basis  $\{|i\rangle\}_{i=1,\dots,d_A}$  for  $\mathcal{H}_A$  and an orthonormal basis for  $\mathcal{L}(\mathcal{H}_E)$ . Let  $\rho_A \in \mathcal{L}(\mathcal{H}_A)$  be classical with respect to the fixed basis of  $\mathcal{H}_A$ . Let  $\mathcal{T}_{A \rightarrow E}$  be a linear map from  $\mathcal{L}(\mathcal{H}_A)$  to  $\mathcal{L}(\mathcal{H}_E)$  that preserves the diagonal structure of the input state (i.e. it is classical). The classical diamond norm of  $\mathcal{T}_{A \rightarrow E}$  is defined to be:

$$\|\mathcal{T}_{A \rightarrow E}\|_{\diamond}^{cl} := \max_{\rho_A} \frac{\|\mathcal{T}_{A \rightarrow E}(\rho_A)\|_1}{\|\rho_A\|_1}.$$

The notion of “classicality” is basis dependent. Thus the above is not a good norm in the sense of operator norms. Nevertheless once a basis is chosen it can be seen as a classical analogue of the diamond norm. Moreover note that there is no notion of “entanglement” in the classical case, such that one can leave out the tensoring with the operator identity typical for the diamond norm in this case without changing the value of the norm. Finally we state an alternative definition of a  $k$ -wise almost independent family of permutations.

**Definition 16.** Let  $\mathcal{P}_W$  and  $\mathcal{P}_H$  be as in Definition 14.  $\mathcal{P}_W$  is called an  $\varepsilon$ -almost  $k$ -wise independent family of permutations if and only if

$$\|\mathcal{P}_W - \mathcal{P}_H\|_1^{cl} \leq \varepsilon.$$

This definition strongly resembles the definition of a unitary  $\varepsilon$ -almost  $k$ -design. Indeed one can see it as a classical motivation for the quantum mechanical definition of an almost  $k$ -design. In the next subsection we proof the consistency of the two different definitions of almost independent families of permutations (Definitions 13 and 16), i. e. we show that  $\mathcal{P}_W$  is an  $\varepsilon$ -almost  $k$ -wise independent family of permutations (with respect to Definition 16) if and only if the underlying set  $\mathcal{F}$  is  $k$ -wise almost independent (according to Definition 13). Afterwards in a short subsection we give a concrete example of pairwise independent family of permutations.

### 6.1.1 Proving the equivalence of the two different views on almost independent families of permutations

For the proof we consider the case of pairwise independent families of permutations but the discussion can be generalized to  $k > 2$  in a straight forward manner.

Assume that  $\mathcal{F}$  is an  $\varepsilon$ -almost independent family of permutations according to Definition 13. We now that choosing a permutation uniformly at random from  $\mathcal{F}$  induces a probability distribution on  $[N_2]$  that is close to the uniform one. Formalizing this statement, we get

$$\sum_{\omega \in [N_2]} \left| \text{Prob}_{P \in \mathcal{F}} [(Px_1, Px_2) = \omega] - \text{Prob}_{P \in \mathfrak{P}} [(Px_1, Px_2) = \omega] \right| \leq \varepsilon \quad \forall (x_1, x_2) \in [N_2], \quad (6.2)$$

where  $\text{Prob}_{P \in \mathcal{F}} [(Px_1, Px_2) = \omega]$  denotes the probability that choosing  $P \in \mathcal{F}$  uniformly at random for a fixed element  $(x_1, x_2) \in [N_2]$  we get  $(Px_1, Px_2) = \omega$ . Similarly  $\text{Prob}_{P \in \mathfrak{P}} [(Px_1, Px_2) = \omega]$  is defined but in this case  $P$  is chosen uniformly at random from  $\mathfrak{P}$ . Note that  $\text{Prob}_{P \in \mathfrak{P}} [(Px_1, Px_2) = \omega]$  is constant and thus corresponds to the uniform distribution over  $[N_2]$ . The above can be translated into the language of quantum mechanics introducing the classical density operators  $\rho$  and  $\sigma$  with

$$\rho := \sum_{\omega \in [N_2]} \text{Prob}_{P \in \mathcal{F}} [(Px_1, Px_2) = \omega] |\omega\rangle\langle\omega| \quad (6.3)$$

$$\sigma := \sum_{\omega \in [N_2]} \text{Prob}_{P \in \mathfrak{P}} [(Px_1, Px_2) = \omega] |\omega\rangle\langle\omega|. \quad (6.4)$$

and equation (6.2) is equivalently rewritten as

$$\|\rho - \sigma\|_1 \leq \varepsilon \quad \forall (x_1, x_2) \in [N_2] \quad (6.5)$$

since the Schatten 1-norm of some matrix is given by the sum of the absolute eigenvalues of this matrix. To represent a classical  $n$ -bit string in a quantum mechanical language, we enumerate each bit string of length  $n$  by a number  $i \in \{1, \dots, 2^n\}$ . Then we choose the canonical basis  $\{e_i\}_{i \in \{1, \dots, 2^n\}}$  of a  $2^n$ -dimensional Hilbert space  $\mathcal{H}$  and identify the  $i$ -th bit-string with the  $i$ -th basis vector. As a result to each of the  $(2^n)!$  permutations in  $\mathfrak{P}$  corresponds a unique permutation operator in  $\mathbb{P}$ . The vector  $|\omega\rangle$  is an element of a bipartite Hilbert space, because  $\omega = (y_1, y_2) \in [N_2]$  and each  $y_i$  corresponds to an element of the canonical basis of  $\mathcal{H}$ .

Strictly speaking the density operator  $\rho$  defined in equation (6.3) should have an index  $(x_1, x_2)$  since it is dependent on the “input”  $(x_1, x_2)$ . We will keep this fact in mind. Let  $e_1$  and  $e_2$  be the quantum mechanical representations of the strings  $x_1, x_2$ . We can rewrite  $\rho$  with a slight abuse of notation as

$$\rho = \sum_{\omega \in [N_2]} \text{Prob}_{P \in \mathcal{F}} [(Px_1, Px_2) = \omega] |\omega\rangle\langle\omega| \quad (6.6)$$

$$= \sum_{\omega \in [N_2]} \text{Prob}_{P \in \mathcal{F}} [(P \otimes P)|e_1\rangle \otimes |e_2\rangle = |\omega\rangle] |\omega\rangle\langle\omega|. \quad (6.7)$$

The set  $\mathcal{F}$  is meant to be once a subset of  $\mathfrak{P}$  and once of  $\mathbb{P}$ . But since there is a one to one correspondence between the elements of these sets as described above, the notation is still well defined. Furthermore we have

$$\begin{aligned} & \sum_{\omega \in [N_2]} \text{Prob}_{P \in \mathcal{F}} [(P \otimes P)|e_1\rangle \otimes |e_2\rangle = |\omega\rangle] |\omega\rangle\langle\omega| \\ &= \sum_{\omega \in [N_2]} \left( \sum_{\substack{P \in \mathcal{F} \\ (P \otimes P)|e_1\rangle \otimes |e_2\rangle = |\omega\rangle}} \frac{1}{|\mathcal{F}|} \right) |\omega\rangle\langle\omega| \end{aligned} \quad (6.8)$$

$$= \sum_{\omega \in [N_2]} \left( \sum_{\substack{P \in \mathcal{F} \\ (P \otimes P)|e_1\rangle \otimes |e_2\rangle = |\omega\rangle}} \frac{1}{|\mathcal{F}|} (P \otimes P)|e_1 \otimes e_2\rangle\langle e_1 \otimes e_2|(P \otimes P)^\dagger \right) \quad (6.9)$$

$$= \sum_{P \in \mathcal{F}} \frac{1}{|\mathcal{F}|} (P \otimes P)|e_1 \otimes e_2\rangle\langle e_1 \otimes e_2|(P \otimes P)^\dagger. \quad (6.10)$$

An identical calculation shows that

$$\sigma = \sum_{P \in \mathbb{P}} \frac{1}{|\mathbb{P}|} (P \otimes P)|e_1 \otimes e_2\rangle\langle e_1 \otimes e_2|(P \otimes P)^\dagger \quad (6.11)$$

and reveals that the condition (6.2) is equivalent to

$$\|\mathcal{P}_W(|e_1 \otimes e_2\rangle\langle e_1 \otimes e_2|) - \mathcal{P}_H(|e_1 \otimes e_2\rangle\langle e_1 \otimes e_2|)\|_1 \leq \varepsilon \quad \forall |e_1 \otimes e_2\rangle; e_1 \neq e_2, \quad (6.12)$$

where the functions  $\mathcal{P}_W$  and  $\mathcal{P}_H$  are as in Definition 14 for  $k = 2$ . If  $\mathcal{F}$  (or in other words  $\mathcal{P}_W$ ) is a pairwise almost independent family of permutations according to Definition 16, then the derivation of equation (6.12) implies that it is also such a family with respect to Definition 13. On the other hand if  $\mathcal{F}$  is a pairwise almost independent family of permutations according to Definition 13 statement (6.12) is always valid. Then for any bipartite classical density operator with  $\sum_{i,j} p_{ij} \leq 1$

$$\zeta := \sum_{i,j} p_{ij} |ij\rangle\langle ij| \quad (6.13)$$

by several applications of the triangle inequality one gets that

$$\begin{aligned} & \|\mathcal{P}_W(\zeta) - \mathcal{P}_H(\zeta)\|_1 \\ &= \left\| \sum_{i,j} p_{ij} (\mathcal{P}_W(|ij\rangle\langle ij|) - \mathcal{P}_H(|ij\rangle\langle ij|)) \right\|_1 \end{aligned} \quad (6.14)$$

$$\leq \left\| \sum_{i \neq j} p_{ij} (\mathcal{P}_W(|ij\rangle\langle ij|) - \mathcal{P}_H(|ij\rangle\langle ij|)) \right\|_1 + \left\| \sum_i p_{ii} (\mathcal{P}_W(|ii\rangle\langle ii|) - \mathcal{P}_H(|ii\rangle\langle ii|)) \right\|_1 \quad (6.15)$$

$$\leq \sum_{i \neq j} p_{ij} \|\mathcal{P}_W(|ij\rangle\langle ij|) - \mathcal{P}_H(|ij\rangle\langle ij|)\|_1 + \sum_i p_{ii} \|\mathcal{P}_W(|ii\rangle\langle ii|) - \mathcal{P}_H(|ii\rangle\langle ii|)\|_1 \quad (6.16)$$

$$\leq \sum_{i \neq j} p_{ij} \varepsilon + \sum_i p_{ii} \|\mathcal{P}_W(|ii\rangle\langle ii|) - \mathcal{P}_H(|ii\rangle\langle ii|)\|_1 \quad (6.17)$$

To bound the first term of (6.16) we used the inequality (6.12) directly. But the second summand has to be bound separately since for (6.12) we require the condition  $i \neq j$ . We do this with a short reformulation, whereby we introduce an arbitrary element of the basis  $|j\rangle \neq |i\rangle$ :

$$\begin{aligned} & \|\mathcal{P}_W(|ii\rangle\langle ii|) - \mathcal{P}_H(|ii\rangle\langle ii|)\|_1 \\ &= \left\| \sum_{P \in \mathcal{F}} \frac{1}{|\mathcal{F}|} (P \otimes P) |ii\rangle\langle ii| (P \otimes P)^\dagger - \sum_{P \in \mathbb{P}} \frac{1}{|\mathbb{P}|} (P \otimes P) |ii\rangle\langle ii| (P \otimes P)^\dagger \right\|_1 \end{aligned} \quad (6.18)$$

$$= \left\| \sum_{P \in \mathcal{F}} \frac{1}{|\mathcal{F}|} P |i\rangle\langle i| P^\dagger - \sum_{P \in \mathbb{P}} \frac{1}{|\mathbb{P}|} P |i\rangle\langle i| P^\dagger \right\|_1 \quad (6.19)$$

$$= \left\| \sum_{P \in \mathcal{F}} \frac{1}{|\mathcal{F}|} P |i\rangle\langle i| P^\dagger \left( \sum_k \langle k|P|j\rangle\langle j|P^\dagger|k\rangle \right) - \sum_{P \in \mathbb{P}} \frac{1}{|\mathbb{P}|} P |i\rangle\langle i| P^\dagger \left( \sum_k \langle k|P|j\rangle\langle j|P^\dagger|k\rangle \right) \right\|_1 \quad (6.20)$$

$$= \left\| \text{tr}_2 \left( \sum_{P \in \mathcal{F}} \frac{1}{|\mathcal{F}|} (P \otimes P) |ij\rangle\langle ij| (P \otimes P)^\dagger - \sum_{P \in \mathbb{P}} \frac{1}{|\mathbb{P}|} (P \otimes P) |ij\rangle\langle ij| (P \otimes P)^\dagger \right) \right\|_1 \quad (6.21)$$

$$\leq \left\| \sum_{P \in \mathcal{F}} \frac{1}{|\mathcal{F}|} (P \otimes P) |ij\rangle\langle ij| (P \otimes P)^\dagger - \sum_{P \in \mathbb{P}} \frac{1}{|\mathbb{P}|} (P \otimes P) |ij\rangle\langle ij| (P \otimes P)^\dagger \right\|_1 \quad (6.22)$$

$$\leq \varepsilon \quad (6.23)$$

In equation (6.20) both bracket terms are equal one and there exists always a vector  $|j\rangle \neq |i\rangle$  (in all nontrivial cases). With the partial trace in (6.21) we mean that we trace out the second system and we use the monotonicity of the trace distance under



TPCPM for the following inequality. We plug this result into equation (6.17) to find

$$\|\mathcal{P}_W(\zeta) - \mathcal{P}_H(\zeta)\|_1 \leq \sum_{i \neq j} p_{ij} \varepsilon + \sum_i p_{ii} \varepsilon \quad (6.24)$$

$$\leq \varepsilon. \quad (6.25)$$

If  $\mathcal{F}$  is a pairwise  $\varepsilon$ -almost independent family of permutations according to Definition 13 inequality (6.12) is satisfied and subsequently (6.25) is valid for any classical  $\zeta$ . This implies that  $\mathcal{F}$  is an  $\varepsilon$ -almost independent family with respect to Definition 16, which concludes the proof of the equivalence of the two different definitions.

### 6.1.2 An exemplary pairwise independent family of permutations

We would like to give a concrete example of a family of pairwise independent permutations. Choose the set  $\{0, 1\}^n$  of  $n$ -bit strings. Give it the structure of a field,  $GF(2^n)$ , introducing the entrywise addition and multiplication operations (mod 2).

**Proposition:** *The family  $\mathcal{F} := \{P_{a,b} \mid a, b \in GF(2^n) \wedge a \neq 0\}$  of permutations defined via*

$$\begin{aligned} P_{a,b} : GF(2^n) &\rightarrow GF(2^n) \\ x &\mapsto P_{a,b}(x) := a \cdot x + b \end{aligned}$$

*is pairwise independent.*

First note that if choosing  $x_1, x_2 \in GF(2^n)$  with  $x_1 \neq x_2$  they are mapped to distinct elements  $y_1 := P_{a,b}(x_1)$  and  $y_2 := P_{a,b}(x_2)$  by any element of the family  $\mathcal{F}$ . This is because we have by assumption that  $a \neq 0$  and the addition in a field is a bijective map. Thus the maps  $P_{a,b}$  can be seen as maps from  $[N_2]$  into itself. Choosing  $(a, b)$  uniformly at random from  $(GF(2^n) - \{0\}) \times GF(2^n)$  corresponds to the choice of a permutation uniformly at random from  $\mathcal{F}$ . To see that the induced distribution on  $[N_2]$  is uniform, we check that for any input  $(x_1, x_2) \in [N_2]$  each pair  $(y_1, y_2)$  is hit with equal probability:

$$a \cdot x_1 + b = y_1 \quad (6.26)$$

$$a \cdot x_2 + b = y_2 \quad (6.27)$$

This is equivalent to

$$\begin{pmatrix} x_1 & 1 \\ x_2 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, \quad (6.28)$$

where the condition  $x_1 \neq x_2$  implies that

$$\det \begin{pmatrix} x_1 & 1 \\ x_2 & 1 \end{pmatrix} \neq 0. \quad (6.29)$$

Thus for any  $(y_1, y_2) \in [N_2]$  there exists a unique  $P_{a,b} \in \mathcal{F}$  with

$$P_{a,b}(x_1) = y_1 \quad (6.30)$$

$$P_{a,b}(x_2) = y_2 \quad (6.31)$$

which implies that the induced distribution is uniform.

## 6.2 CQ-decoupling theorem for pairwise $\varepsilon$ -dependent families of permutations

We generalize the CQ-decoupling theorem for the partial trace derived in Section 5.3 in the sense that we only average over a  $\varepsilon$ -almost pairwise independent family of permutations. This can be seen as an example. It is also possible to generalize the results of the Sections 5.4 and 5.5 in the same sense but we won't do that explicitly since the derivations strongly resemble this chapter's discussion.

**Theorem:** (CQ-Decoupling Theorem for the Partial Trace) *Let  $\rho_{\text{AR}}$  be classical on  $\mathcal{H}_A$  with respect to  $\{|i\rangle\}_{i=1,\dots,d_A}$  and let  $A = (A_1 A_2)$  be a composite system, then the average distance from uniform is given by*

$$\begin{aligned} & \frac{1}{|\mathcal{F}|} \sum_{P_A \in \mathcal{F}} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \rho_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1 \\ & \leq \sqrt{d_{A_1} \left( \frac{d_A - d_{A_2}}{d_A - 1} + 4\varepsilon d_A \right) 2^{-H_2(A|R)_\rho}}, \end{aligned}$$

where the average goes over a family  $\mathcal{F}$  of pairwise  $\varepsilon$ -almost independent permutation operators, which act by permuting the basis vectors of  $\{|i\rangle\}_{i=1,\dots,d_A}$ .

By an application of (5.53) we get that

$$\begin{aligned} & \frac{1}{|\mathcal{F}|} \sum_{P_A \in \mathcal{F}} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1^2 \\ & \leq d_{A_1} \frac{1}{|\mathcal{F}|} \sum_{P_A \in \mathcal{F}} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \tilde{\rho}_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \tilde{\rho}_R \right\|_2^2 \end{aligned} \quad (6.32)$$

$$= d_{A_1} \frac{1}{|\mathcal{F}|} \sum_{P_A \in \mathcal{F}} \text{tr} \left( \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R (\tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R) P_A^\dagger \otimes \mathbb{1}_R)^2 \right) \quad (6.33)$$

$$= d_{A_1} \frac{1}{|\mathcal{F}|} \sum_{P_A \in \mathcal{F}} \text{tr} \left( ((P_A \otimes \mathbb{1}_R)^{\otimes 2} (\tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R)^{\otimes 2} (P_A^\dagger \otimes \mathbb{1}_R)^{\otimes 2}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1}) \otimes \mathcal{F}_R \right). \quad (6.34)$$

The (indefinite) operator  $\tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R$  has CQ-structure. It can be written as

$$\tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R = \sum_i |i\rangle\langle i|_A \otimes \tilde{\rho}_R^{[i]} - \sum_i |i\rangle\langle i|_A \otimes \frac{1}{d_A} \tilde{\rho}_R \quad (6.35)$$

$$= \sum_i |i\rangle\langle i|_A \otimes \left( \tilde{\rho}_R^{[i]} - \frac{1}{d_A} \tilde{\rho}_R \right) \quad (6.36)$$

$$=: \sum_i |i\rangle\langle i|_A \otimes \tilde{\mu}_R^{[i]}. \quad (6.37)$$

Then (omitting the pre-factor) equation (6.34) becomes

$$\begin{aligned} & \frac{1}{|\mathcal{F}|} \sum_{P_A \in \mathcal{F}} \text{tr} \left( ((P_A \otimes \mathbb{1}_R)^{\otimes 2} (\tilde{\rho}_{AR} - \pi_A \otimes \tilde{\rho}_R)^{\otimes 2} (P_A^\dagger \otimes \mathbb{1}_R)^{\otimes 2}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1}) \otimes \mathcal{F}_R \right) \\ & = \frac{1}{|\mathcal{F}|} \sum_{i,j} \sum_{P_A \in \mathcal{F}} \text{tr} \left( (P_A |i\rangle\langle i|_A P_A^\dagger \otimes P_A |j\rangle\langle j|_{A'} P_A^\dagger) \otimes \tilde{\mu}_R^{[i]} \otimes \tilde{\mu}_R^{[j]} (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1}) \otimes \mathcal{F}_R \right) \end{aligned} \quad (6.38)$$

$$\begin{aligned} & = \sum_{i,j} \text{tr} \left( ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) \otimes \tilde{\mu}_R^{[i]} \otimes \tilde{\mu}_R^{[j]}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1}) \otimes \mathcal{F}_R \right) \\ & \quad + \sum_{i,j} \text{tr} \left( (\mathcal{P}_H(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) \otimes \tilde{\mu}_R^{[i]} \otimes \tilde{\mu}_R^{[j]}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1}) \otimes \mathcal{F}_R \right). \end{aligned} \quad (6.39)$$

We added and subtracted the term  $\mathcal{P}_H(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'})$  in the last step. This allows for an application of the defining property of the  $\varepsilon$ -almost pairwise independent family of permutations in the first term of (6.39). The second term in equation (6.39) is bounded in Section 5.3. As was already the case when we considered decoupling with  $\varepsilon$ -almost unitary 2-designs, this term corresponds to taking the average over the whole group. Thus in our case it is just one of the intermediate equations in the derivation of the CQ-Decoupling Theorem for Partial Trace. We will add the contribution of

the second term in the end of the derivation but now we focus our attention to the first term. A short reformulation shows that

$$\begin{aligned} & \sum_{i,j} \text{tr} \left( ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) \otimes \tilde{\mu}_R^{[i]} \otimes \tilde{\mu}_{R'}^{[j]}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1}) \otimes \mathcal{F}_R \right) \\ &= \sum_{i,j} \text{tr} ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})) \text{tr} \left( \tilde{\mu}_R^{[i]} \otimes \tilde{\mu}_{R'}^{[j]} \mathcal{F}_R \right) \end{aligned} \quad (6.40)$$

$$= \sum_{i,j} \text{tr} ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})) \text{tr} \left( \tilde{\mu}_R^{[i]} \tilde{\mu}_{R'}^{[j]} \right). \quad (6.41)$$

We bound the trace term with the Schatten 1-norm to find that

$$\begin{aligned} & \text{tr} ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})) \\ & \leq \|(\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})\|_1 \end{aligned} \quad (6.42)$$

$$\leq \|(\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'})\|_1 \|(\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})\|_\infty \quad (6.43)$$

$$= \|(\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'})\|_1 \quad (6.44)$$

$$\leq \varepsilon. \quad (6.45)$$

For the last step we used the fact that  $\mathcal{P}_W$  constitutes an  $\varepsilon$ -almost pairwise independent family of permutations together with the results of the discussion of Section 6.1.1. In a similar manner one shows that

$$(-\varepsilon) \leq \text{tr}((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})). \quad (6.46)$$

To see where the upper bound and where the lower bound is required we write out the  $\tilde{\mu}_R^{[i]}$  and  $\tilde{\mu}_{R'}^{[j]}$  in equation (6.41) and get

$$\begin{aligned} & \sum_{i,j} \text{tr} ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})) \text{tr} \left( \tilde{\mu}_R^{[i]} \tilde{\mu}_{R'}^{[j]} \right) \\ &= \sum_{i,j} \text{tr} ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})) \text{tr} \left( \tilde{\rho}_R^{[i]} \tilde{\rho}_{R'}^{[j]} \right) \\ & \quad - \frac{1}{d_A} \sum_{i,j} \text{tr} ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})) \text{tr} \left( \tilde{\rho}_R^{[i]} \tilde{\rho}_R \right) \\ & \quad - \frac{1}{d_A} \sum_{i,j} \text{tr} ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})) \text{tr} \left( \tilde{\rho}_R \tilde{\rho}_R^{[i]} \right) \\ & \quad + \frac{1}{d_A^2} \sum_{i,j} \text{tr} ((\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_{A'}) (\mathbb{1}_{A_2 A'_2} \otimes \mathcal{F}_{A_1 A'_1})) \text{tr} (\tilde{\rho}_R \tilde{\rho}_{R'}) \end{aligned} \quad (6.47)$$

$$\leq \varepsilon \cdot \sum_{i,j} \text{tr} \left( \tilde{\rho}_R^{[i]} \tilde{\rho}_R^{[j]} \right) + \varepsilon \cdot \frac{2}{d_A} \sum_{i,j} \text{tr} \left( \tilde{\rho}_R^{[i]} \tilde{\rho}_R \right) + \varepsilon \cdot \frac{1}{d_A^2} \sum_{i,j} \text{tr} (\tilde{\rho}_R \tilde{\rho}_R) \quad (6.48)$$

$$= 4\varepsilon \cdot \text{tr} (\tilde{\rho}_R \tilde{\rho}_R). \quad (6.49)$$

Equation (6.49) makes use of the CQ-structure of  $\rho_{\text{AR}}$ . Note that the partial trace  $\tilde{\rho}_{\text{R}}$  of  $\tilde{\rho}_{\text{AR}}$  is given by  $\tilde{\rho}_{\text{R}} = \sum_i \tilde{\rho}_{\text{R}}^{[i]}$ . An application of the Cauchy-Schwarz inequality shows that

$$\text{tr}(\tilde{\rho}_{\text{R}}^2) = \text{tr}(\tilde{\rho}_{\text{AR}} \otimes \mathbb{1}_{\text{A}'} \tilde{\rho}_{\text{A}'\text{R}} \otimes \mathbb{1}_{\text{A}}) \quad (6.50)$$

$$\leq \sqrt{\text{tr}((\tilde{\rho}_{\text{AR}} \otimes \mathbb{1}_{\text{A}'})^2) \text{tr}((\tilde{\rho}_{\text{A}'\text{R}} \otimes \mathbb{1}_{\text{A}})^2)} \quad (6.51)$$

$$= d_{\text{A}} \text{tr}(\tilde{\rho}_{\text{AR}}^2). \quad (6.52)$$

This bound is very bad since it does not use the given CQ-structure of  $\tilde{\rho}_{\text{AR}}$  but until now, I was not able to find a significantly better bound (i.e. a bound that does not involve any dimension factors). With equation (6.49) this yields a bound on the first term of (6.39)

$$\begin{aligned} & \sum_{i,j} \text{tr} \left( \left( (\mathcal{P}_W - \mathcal{P}_H)(|i\rangle\langle i|_{\text{A}} \otimes |j\rangle\langle j|_{\text{A}'}) \otimes \tilde{\mu}_{\text{R}}^{[i]} \otimes \tilde{\mu}_{\text{R}'}^{[j]} \right) (\mathbb{1}_{\text{A}_2\text{A}'_2} \otimes \mathcal{F}_{\text{A}_1\text{A}'_1}) \otimes \mathcal{F}_{\text{R}} \right) \\ & \leq 4\varepsilon d_{\text{A}} \text{tr}(\tilde{\rho}_{\text{AR}}^2). \end{aligned} \quad (6.53)$$

The bound on the second term of (6.39) is

$$\sum_{i,j} \text{tr} \left( \mathcal{P}_H(|i\rangle\langle i|_{\text{A}} \otimes |j\rangle\langle j|_{\text{A}'}) \otimes \tilde{\mu}_{\text{R}}^{[i]} \otimes \tilde{\mu}_{\text{R}'}^{[j]} (\mathbb{1}_{\text{A}_2\text{A}'_2} \otimes \mathcal{F}_{\text{A}_1\text{A}'_1}) \otimes \mathcal{F}_{\text{R}} \right) \leq \frac{d_{\text{A}} - d_{\text{A}_2}}{d_{\text{A}} - 1} \text{tr}(\tilde{\rho}_{\text{AR}}^2). \quad (6.54)$$

We conclude taking together both results that

$$\begin{aligned} & \frac{1}{|\mathcal{F}|} \sum_{P_{\text{A}} \in \mathcal{F}} \left\| \text{tr}_{\text{A}_2}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} \rho_{\text{AR}} P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}}) - \pi_{\text{A}_1} \otimes \rho_{\text{R}} \right\|_1^2 \\ & \leq d_{\text{A}_1} \left( \frac{d_{\text{A}} - d_{\text{A}_2}}{d_{\text{A}} - 1} \text{tr}(\tilde{\rho}_{\text{AR}}^2) + 4\varepsilon d_{\text{A}} \text{tr}(\tilde{\rho}_{\text{AR}}^2) \right). \end{aligned} \quad (6.55)$$

As always one adjusts the  $\zeta_{\text{R}}$  in  $\tilde{\rho}_{\text{AR}}^2$  to get the  $H_2$ -entropy. Then the square root is taken on both sides followed by an application of the Jensen inequality to find that

$$\begin{aligned} & \frac{1}{|\mathcal{F}|} \sum_{P_{\text{A}} \in \mathcal{F}} \left\| \text{tr}_{\text{A}_2}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} \rho_{\text{AR}} P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}}) - \pi_{\text{A}_1} \otimes \rho_{\text{R}} \right\|_1 \\ & \leq \sqrt{d_{\text{A}_1} \left( \frac{d_{\text{A}} - d_{\text{A}_2}}{d_{\text{A}} - 1} + 4\varepsilon d_{\text{A}} \right) 2^{-H_2(\text{A}|\text{R})_{\rho}}}. \end{aligned} \quad (6.56)$$

## Chapter 7

# Decoupling Quantum States with Permutation Operators

The aim of this chapter is to understand whether permutations operators can be used for decoupling applications in a quantum context. We would like to generalize the discussion of Chapter 5 dropping the assumption that the state of the system has CQ-structure.

This chapter requires a solid understanding of the representation theory of the symmetric group  $S_d$ . An introduction to this topic is beyond the scope of this project but can be found in [18].

### 7.1 The general setup

Instead of bounding the term

$$\int_{\mathbb{U}(A)} \left\| \mathcal{T}(U_A \otimes \mathbb{1}_R \rho_{AR} U_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_1 dU \quad (7.1)$$

as is done in the Decoupling Theorem, one might be interested in an upper bound on expressions of the type

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \omega_E \otimes \rho_R \right\|_1. \quad (7.2)$$

It turns out that for arbitrary  $\rho_{AR}$  and  $\mathcal{T}_{A \rightarrow E}$  the computational effort required for the solution of this problem is big. Moreover the occurring bounds are difficult to interpret in terms of entropies. Nevertheless the presented method is general in the sense that it can be used to obtain upper bounds on (7.2) for any  $\rho_{AR}$  and any  $\mathcal{T}_{A \rightarrow E}$ . It even allows to bound the distance from states different than  $\omega_R \otimes \rho_R$ . Generally the calculations in this section will be very close to the calculations done in the proof

of the Decoupling Theorem. Conceptually we therefore can follow the discussion of Chapter 2. We will study three variations of formula (7.2) in this thesis, which we consider to be interesting. The first one shows how much classicalizing a map can be made by a pre-concatenation of a permutation operator. We prove

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R (\Phi_{AR} - T_{AR}) P_A^\dagger \otimes \mathbb{1}_R) \right\|_1 \leq \sqrt{d_A \frac{d_R - 1}{d_A - 1} 2^{-H_{\min}(A|E)_\omega}},$$

where we define  $\Phi_{AR} := \frac{1}{d_R} \sum_{i,j} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_R$  and  $T_{AR} := \frac{1}{d_R} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_R$ . The second one is an important special case of a general decoupling theorem with permutations. There we bound

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R (\Phi_{AR} - \pi_{AR}) P_A^\dagger \otimes \mathbb{1}_R) \right\|_1 \leq \sqrt{2 \frac{d_A^2}{d_R} \frac{d_R - 1}{d_A - 1} 2^{-H_{\min}(A|E)_\omega}},$$

where  $\Phi_{AR}$  is defined as above and  $\pi_{AR} := \frac{1}{d_R^2} \sum_{i,j} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_R$ . Finally we generalize on the discussion of Section 5.2 dropping the assumption that the  $A$  system is classical. This provides us with a generalization of the Hash Lemma (as stated for instance in [21]) to the fully quantum context. We obtain that

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \text{tr}_{A_2}(P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1 \leq \sqrt{2 d_{A_1} 2^{-H_{\min}(A|R)_\rho}}.$$

The structure of the derivations is as always. We first derive “decoupling lemmata”, where instead of the Schatten 1-norm, the above expressions contain the Schatten 2-norm. Then we use the Hölder inequality to go to the Schatten 1-norm and to obtain bounds in terms of entropic quantities. Finally the Jensen Inequality is applied and we lower bound the different entropies with the  $H_{\min}$ -entropy. Since we would like to study two different special cases we keep the discussion completely general for the moment. We will specialize to the above cases as soon as this becomes necessary. To

keep the discussion general we introduce the hermitian operator  $\lambda_{\text{AR}}$  and write

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R \lambda_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_R) \right\|_2^2 \\ &= \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \text{tr} \left( \mathcal{T}(P_A \otimes \mathbb{1}_R \lambda_{\text{AR}} P_A^\dagger \otimes \mathbb{1}_R)^2 \right) \end{aligned} \quad (7.3)$$

$$= \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \text{tr} \left( \mathcal{T}^{\otimes 2} \left( (P_A \otimes \mathbb{1}_R)^{\otimes 2} (\lambda_{\text{AR}})^{\otimes 2} (P_A^\dagger \otimes \mathbb{1}_R)^{\otimes 2} \right) \mathcal{F}_{\text{ER}} \right) \quad (7.4)$$

$$= \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \text{tr} \left( (\lambda_{\text{AR}})^{\otimes 2} \left( (P_A^\dagger)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{E}}] (P_A)^{\otimes 2} \right) \otimes \mathcal{F}_{\text{R}} \right) \quad (7.5)$$

$$= \text{tr} \left( (\lambda_{\text{AR}})^{\otimes 2} \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left( (P_A^\dagger)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{E}}] (P_A)^{\otimes 2} \right) \otimes \mathcal{F}_{\text{R}} \right). \quad (7.6)$$

The evaluation of the term

$$\sum_{P \in \mathbb{P}(A)} \left( (P_A^\dagger)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{E}}] (P_A)^{\otimes 2} \right) = \sum_{P \in \mathbb{P}(A)} \left( (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{E}}] (P_A^\dagger)^{\otimes 2} \right) \quad (7.7)$$

constitutes the major part of this chapter and is performed in the following section.

## 7.2 The mathematical backbone for decoupling theorems with permutations

This section is partitioned in five subsections in which we present different ingredients, which taken together will allow us to calculate  $\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{E}}] (P_A^\dagger)^{\otimes 2}$ . The first subsection introduces some basic notions from representation theory and shows how they are related to our problem. The following three subsections deal with the analysis of the commutant of a given representation and specialize this to our concrete example. In the last subsection we compute  $\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_{\text{E}}] (P_A^\dagger)^{\otimes 2}$ . The rest of this chapter is then organized in two further sections, “Distance from classicality” and “Decoupling with permutation operators”, in which we apply the result of this section.

### 7.2.1 Basics from representation theory

As already mentioned in the beginning an introduction to the area of representation theory cannot be given in this thesis. Nevertheless it is inevitable to introduce some notational conventions and fix the terminology of the following subsections.



Any element  $\sigma$  of the symmetric group  $S_d$  can be written in *cycle notation*. There, a permutation is represented by a sequence of cycles  $(\dots)(\dots)\dots(\dots)$  with each cycle containing a sequence of elements of  $\{1, \dots, d\}$ . Each entry of a cycle is mapped by the corresponding permutation to the following entry in the cycle. The last entry of a cycle is mapped to its first one. For instance the cycle  $(i\ j\ k)$  corresponds to a permutation in  $S_3$  that maps  $i$  to  $j$ ,  $j$  to  $k$  and  $k$  back to  $i$ . For a given permutation one can count the different cycles in it. We call the tuple  $((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$  the *cycle structure* of a permutation with  $k_1$  cycles of length one,  $k_2$  cycles of length two etc. Note that the integers  $k_i$  are constrained to satisfy  $\sum_i i k_i = d$ . It is easy to show that the cycle structure of some permutation in  $S_d$  is invariant under the conjugation of this permutation with an arbitrary element of  $S_d$ . Two permutations are in the same conjugacy class if and only if their cycle structure is the same. It is therefore possible to label the conjugacy classes of  $S_d$  by tuples  $((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$ . Furthermore, we call a non increasing sequence of natural numbers  $\lambda = (\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n)$  with  $\sum_i \lambda_i = d$  a *partition* of  $d$ . From the above labeling of conjugacy classes of  $S_d$  we see that it is alternatively possible to label these classes via partitions of  $d$ . A function from a group into some field which is constant on each conjugacy class of that group is called a *class function*.

An extremely important concept in Quantum Mechanics is the one of representing the action of some group (as for example  $S_d$ ) on a vector space.

**Definition 17.** (Representation) Let  $V$  be a  $d$ -dimensional  $\mathbb{C}$ -vector space. A (linear) representation of a group  $G$  is a group homomorphism

$$\begin{aligned} X : G &\rightarrow Gl(V) \\ g &\mapsto X(g), \end{aligned}$$

where with  $Gl(V)$  we denote the General Linear Group of invertible linear maps from  $V$  onto itself.

In our context it will often be sufficient to fix a basis for  $V$  and think of the representation as attaching to each group element an invertible  $d \times d$ -matrix. This type of representations will be called matrix representations. We have already seen the defining representation of the group  $S_d$ , which can be seen as a matrix representation assigning to each element  $\sigma \in S_d$  the corresponding permutation operator  $P(\sigma)$  (see Definition 9) via

$$\begin{aligned} P : S_d &\rightarrow Gl(d \times d, \mathbb{C}) \\ \sigma &\mapsto P(\sigma), \end{aligned}$$

where with  $Gl(d \times d, \mathbb{C})$  we denote the group of invertible  $d \times d$ -matrices. Another interesting representation is the *swap representation* of  $S_2$ . For  $V$  being a  $d$ -dimensional vector space one defines

$$S : S_2 \rightarrow Gl(V \otimes V)$$

$$\sigma \mapsto S(\sigma) := \begin{cases} \mathbb{1} & \text{if } \sigma = e \\ \mathcal{F} & \text{otherwise} \end{cases}$$

where we wrote  $e$  for the neutral element of  $S_2$  and  $\mathcal{F}$  is the swap operator on  $V \otimes V$ . In our concrete setup the following representation will be of particular interest. We denote by  $S_d \times S_2$  the group of pairs of elements from  $S_d$  and  $S_2$  and define for  $d$ -dimensional  $V$  the representation

$$R : S_d \times S_2 \rightarrow Gl(V \otimes V)$$

$$(\sigma, \pi) \mapsto R((\sigma, \pi)) := (P(\sigma) \otimes P(\sigma), S(\pi)),$$

where the pair  $(P(\sigma) \otimes P(\sigma), S(\pi))$  acts on  $V \otimes V$  by multiplication: For  $|i\rangle \otimes |j\rangle \in V \otimes V$  one has

$$(P(\sigma) \otimes P(\sigma), S(\pi))(|i\rangle \otimes |j\rangle) := (P(\sigma) \otimes P(\sigma)) \cdot S(\pi)(|i\rangle \otimes |j\rangle). \quad (7.8)$$

Since the actions of  $P(\sigma) \otimes P(\sigma)$  and  $S(\pi)$  commute the representation is well defined. Later we will decompose this representation into irreducible representations of  $S_d \times S_2$ . For this it is convenient to label the irreducible representations of  $S_d$  using partitions of  $d$ . (The irreducible representations are in one to one correspondence to the conjugacy classes of  $S_d$ .) For example we will write  $\pi_{(d-1,1)}$  for the irreducible representation  $\pi$  of  $S_d$  belonging to the partition  $(d-1, 1)$  (or the Young Frame with  $d-1$  boxes in the first row and one box in the second one).

For a given representation we define its “character” and its “commutant”. These objects will be of interest for our problem.

**Definition 18.** (Character [18]) Given a representation  $X$  of  $G$  on a  $\mathbb{C}$ -vectorspace, the character of  $X$  is a map

$$\chi : G \rightarrow \mathbb{C}$$

$$g \mapsto \chi(g) := \text{tr}(X(g)),$$

where the trace is taken of one of the matrices representing the map  $X(g)$ .

The characters are well defined since two different matrices  $A, B$  representing the same linear map from  $V$  into itself are related via  $B = S A S^{-1}$  for some fixed  $S$ . Therefore  $\text{tr}(B) = \text{tr}(A)$ . From the definition it is also clear that characters are class functions.

**Definition 19.** (Commutant [18]) Let  $\text{Mat}(d \times d, \mathbb{C})$  be the set of all  $d \times d$ -matrices with complex entries and let  $Gl(d \times d, \mathbb{C}) \subset \text{Mat}(d \times d, \mathbb{C})$  be the subset of invertible matrices. For a matrix representation  $X : G \rightarrow Gl(d \times d, \mathbb{C})$  the corresponding commutant is

$$\text{Com}(X) = \{T \in \text{Mat}(d \times d, \mathbb{C}) : T \cdot X(g) = X(g) \cdot T \quad \forall g \in G\}.$$

From the definition it is evident that  $\text{Com}(X)$  has the structure of an algebra. We now consider the term

$$\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} = \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} \left( \sum_{i,j} \mathcal{T}^\dagger(|i\rangle\langle j|_A) \otimes \mathcal{T}^\dagger(|j\rangle\langle i|_{A'}) \right) (P_A^\dagger)^{\otimes 2} \quad (7.9)$$

and note that

$$\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} \in \text{Com}(R). \quad (7.10)$$

This is because for any  $(\sigma, \pi) \in S_d \times S_2$  we have that

$$\begin{aligned} R((\sigma, \pi)) & \left( \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} \right) R((\sigma, \pi))^{-1} \\ &= (P(\sigma) \otimes P(\sigma)) \cdot S(\pi) \left( \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} \right) S(\pi)^{-1} \cdot (P(\sigma) \otimes P(\sigma))^{-1} \end{aligned} \quad (7.11)$$

$$= (P(\sigma) \otimes P(\sigma)) \left( \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} \right) (P(\sigma) \otimes P(\sigma))^\dagger \quad (7.12)$$

$$= \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2}. \quad (7.13)$$

In equation (7.12) we used the fact that  $S(\pi)$  is either the identity or the swap operator. The invariance under the conjugation with the identity is trivial whereas one can see from equation (7.9) that the whole sum is symmetric in the systems  $A$  and

$A'$  and therefore it is also invariant under the conjugation with the swap operator. Furthermore in equation (7.13) we used the fact that the summation takes place over all permutation operators. If we multiply a permutation operator with another we still get a permutation operator. The map that corresponds to the left multiplication with a permutation operator is bijective. So the whole sum still goes over all permutation operators.

Moreover the term  $(\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E]$  is hermitian, such that

$$\left( \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} \right)^\dagger = \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} \quad (7.14)$$

holds for the whole sum. We denote by  $\text{Com}(R)^\dagger$  the set of the hermitian matrices in  $\text{Com}(R)$ . This set has the structure of a vector space and

$$\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} \in \text{Com}(R)^\dagger. \quad (7.15)$$

This property strongly restricts the possible results of the summation.

## 7.2.2 The structure of the commutant

We have seen that the commutant of the representation  $R$ ,  $\text{Com}(R)$ , is relevant in our context. In this chapter we first analyze the structure of the commutant of a general representation and then see what are the implications on  $\text{Com}(R)$ .

It is a general fact in representation theory (Maschke's Theorem) that any (finite dimensional, unitary) representation of a finite group can be decomposed into a direct sum of irreducible representations. In particular in case of a matrix representation the matrix  $X(g)$  for any  $g \in G$  can be written as

$$X(g) = \begin{pmatrix} X^{[1]}(g) & 0 & \cdots & 0 \\ 0 & X^{[2]}(g) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & X^{[i]}(g) \end{pmatrix} \quad (7.16)$$

in a basis which corresponds to the invariant subspaces. The matrices  $X^{[j]}(g)$  belong to irreducible sub representations of  $X(g)$  and the block diagonal structure of  $X(g)$  reflects the invariance of the corresponding irreducible subspaces. Thus for any matrix representation there exists a basis in which it can be decomposed into

$$X = \bigoplus_i m_i X^{(i)}, \quad (7.17)$$

where (in contrast to (7.16)) the  $X^{(i)}$  are pairwise inequivalent and have multiplicity  $m_i$ . This fact together with several applications of the fundamental Schur Lemma can be used to show the following theorem about the commutant of some matrix representation.

**Theorem:** (Structure of the commutant ([18] page 26)) *Let  $G$  be a finite group and  $X$  be a (finite dimensional) matrix representation of  $G$ . Assume  $X$  decomposes into inequivalent, irreducible representations as  $X = \bigoplus_i^k m_i X^{(i)}$  and  $X^{(i)}$  has dimension  $d_i$ , then*

$$\text{Com}(X) = \left\{ \bigoplus_i^k (M_{m_i} \otimes \mathbb{1}_{d_i}) \mid M_{m_i} \in \text{Mat}(m_i \times m_i, \mathbb{C}) \right\}$$

The above theorem implies that the dimension of the commutant algebra  $\text{Com}(X)$  only depends on the multiplicities of the irreducible representations occurring in the decomposition of  $X$ . For us in the first place the commutant of  $R$  is interesting. The dimension of  $\text{Com}(R)$  determines the amount of linearly independent matrices in this algebra. We will try to write the term  $\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2}$  as a linear combination of basis vectors of  $\text{Com}(R)^\dagger$ . For this we first determine the dimension  $\dim(\text{Com}(R))$  of  $\text{Com}(R)$ . Finding then the dimension of  $\text{Com}(R)^\dagger$ ,  $\dim(\text{Com}(R)^\dagger)$  is straight forward.

### 7.2.3 The dimension of $\text{Com}(R)^\dagger$

We have seen that the dimension of the commutant  $\text{Com}(R)$  is determined by the multiplicities of the irreducible representation in  $R$ . To obtain these multiplicities we give an explicit decomposition of  $R$  into irreducible representations in terms of characters. We write  $\chi_\lambda$  for the character of the irreducible matrix representation  $X_\lambda$  of  $S_d$  belonging to the conjugacy class  $\lambda$ . Since the irreducible representations of  $S_d \times S_2$  are given by all the tensor products of the irreducible representations of  $S_d$  and  $S_2$  it is possible to label the characters of the irreducible representations of  $S_d \times S_2$  via  $\chi_{\lambda, \mu}$  where  $\mu$  denotes a partition of 2 ([18], Theorem 1.11.3). The character  $\chi_{\lambda, \mu}$  can explicitly be calculated to be  $\chi_{\lambda, \mu} = \chi_\lambda \chi_\mu$  with  $\chi_\lambda$  and  $\chi_\mu$  being characters for  $S_d$  and  $S_2$  respectively.

**Claim:** In the setup of the previous subsection with  $d \geq 4$ , we have for the character  $\chi_R$  of  $R$  that

$$\chi_R = 2 \chi_{(d), (2)} + 2 \chi_{(d-1,1), (2)} + \chi_{(d-1,1), (1,1)} + \chi_{(d-2,1,1), (1,1)} + \chi_{(d-2,2), (2)}.$$

First we give a proof of this claim and afterwards we will see how this result can be used to compute  $\dim(\text{Com}(R)^\dagger)$ . The characters of the irreducible representations of a group form an orthonormal basis for the class functions of that group. The above claim corresponds to an expansion of the class function  $\chi_R$  into that basis. Since generally the coordinates of any vector written in some basis are unique, we conclude that if we can explicitly validate the above expansion, then that decomposition is automatically unique. All characters are class functions and therefore it is sufficient to check the claim on any conjugacy class of  $S_d \times S_2$ . We write a conjugacy class in  $S_d$  in cycle notation labeling it with  $a := ((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$  and a class in  $S_2$  with  $b := ((1)^{l_1}, (2)^{l_2})$ . One can reformulate the claim making the dependence of the functions on the conjugacy classes explicit. Denoting with  $e$  the neutral element of  $S_2$  we get

$$\chi_R(a, b) = \text{tr}(P(a) \otimes P(a) \cdot S(b)) \quad (7.18)$$

$$= \text{tr}(P(a) \otimes P(a)) \delta_{be} + (1 - \delta_{be}) \text{tr}(P(a) \otimes P(a) \mathcal{F}) \quad (7.19)$$

$$= \text{tr}(P(a))^2 \delta_{be} + (1 - \delta_{be}) \text{tr}(P(a)^2) \quad (7.20)$$

$$= k_1^2 \delta_{be} + (1 - \delta_{be}) (k_1 + 2 \cdot k_2). \quad (7.21)$$

$\delta_{be}$  is the function on  $S_2$  which is one on  $e$  and zero else. It can be easily rewritten in terms of the characters of the irreducible representations of  $S_2$ .

$$\delta_{be} = \frac{1}{2} (\chi_{(2)}(b) + \chi_{(1,1)}(b)) \quad (7.22)$$

and

$$1 - \delta_{be} = \frac{1}{2} (\chi_{(2)}(b) - \chi_{(1,1)}(b)), \quad (7.23)$$

which implies that

$$\chi_R(a, b) = \frac{1}{2} k_1^2 (\chi_{(2)}(b) + \chi_{(1,1)}(b)) + \frac{1}{2} (\chi_{(2)}(b) - \chi_{(1,1)}(b)) (k_1 + 2 \cdot k_2). \quad (7.24)$$

The characters on the right hand side of the claim

$$\chi_{(d), (2)}, \chi_{(d-1,1), (2)}, \chi_{(d-1,1), (1,1)}, \chi_{(d-2,1,1), (1,1)}, \chi_{(d-2,2), (2)}$$

can all be evaluated writing them out as products of characters of  $S_d$  and  $S_2$  and afterwards applying the Murnaghan-Nakayama rule ([18], Theorem 4.10.2) to calculate

$$\chi_{(d)}, \chi_{(d-1,1)}, \chi_{(d-2,1,1)} \text{ and } \chi_{(d-2,2)}.$$

It is a conceptually simple but partially elaborate task (see Appendix D) to obtain

$$\chi_{(d)}(a) = 1 \tag{7.25}$$

$$\chi_{(d-1,1)}(a) = k_1 - 1 \tag{7.26}$$

$$\chi_{(d-2,1,1)}(a) = \frac{1}{2} (k_1 - 1)(k_1 - 2) - k_2 \tag{7.27}$$

$$\chi_{(d-2,2)}(a) = \frac{1}{2} k_1(k_1 - 3) + k_2 \tag{7.28}$$

using the Murnaghan-Nakayama rule. With this the right hand side of our claim becomes

$$\begin{aligned} & 2 \chi_{(d),(2)}(a, b) + 2 \chi_{(d-1,1),(2)}(a, b) + \chi_{(d-1,1),(1,1)}(a, b) + \chi_{(d-2,1,1),(1,1)}(a, b) + \chi_{(d-2,2),(2)}(a, b) \\ &= 2 \chi_{(d)}(a) \chi_{(2)}(b) + 2 \chi_{(d-1,1)}(a) \chi_{(2)}(b) + \chi_{(d-1,1)}(a) \chi_{(1,1)}(b) \\ & \quad + \chi_{(d-2,1,1)}(a) \chi_{(1,1)}(b) + \chi_{(d-2,2)}(a) \chi_{(2)}(b) \end{aligned} \tag{7.29}$$

$$\begin{aligned} &= 2 \chi_{(2)}(b) + 2 (k_1 - 1) \chi_{(2)}(b) + (k_1 - 1) \chi_{(1,1)}(b) + \left( \frac{1}{2} (k_1 - 1)(k_1 - 2) - k_2 \right) \chi_{(1,1)}(b) \\ & \quad + \left( \frac{1}{2} k_1(k_1 - 3) + k_2 \right) \chi_{(2)}(b) \end{aligned} \tag{7.30}$$

$$\begin{aligned} &= 2 \chi_{(2)}(b) + 2 (k_1 - 1) \chi_{(2)}(b) + (k_1 - 1) \chi_{(1,1)}(b) + \left( \frac{1}{2} (k_1 - 1)(k_1 - 2) \right) \chi_{(1,1)}(b) \\ & \quad + \left( \frac{1}{2} k_1(k_1 - 3) \right) \chi_{(2)}(b) + \frac{1}{2} (\chi_{(2)}(b) - \chi_{(1,1)}(b)) \cdot (2 k_2) \end{aligned} \tag{7.31}$$

$$\begin{aligned} &= 2 \chi_{(2)}(b) + 2 (k_1 - 1) \chi_{(2)}(b) + (k_1 - 1) \chi_{(1,1)}(b) + \left( \frac{1}{2} k_1^2 - \frac{3}{2} k_1 + 1 \right) \chi_{(1,1)}(b) \\ & \quad + \left( \frac{1}{2} k_1^2 - \frac{3}{2} k_1 \right) \chi_{(2)}(b) + \frac{1}{2} (\chi_{(2)}(b) - \chi_{(1,1)}(b)) \cdot (2 k_2) \end{aligned} \tag{7.32}$$

$$\begin{aligned} &= \frac{1}{2} (\chi_{(2)}(b) + \chi_{(1,1)}(b)) k_1^2 + \frac{1}{2} (\chi_{(2)}(b) - \chi_{(1,1)}(b)) \cdot (2 k_2) \\ & \quad + 2 k_1 \chi_{(2)}(b) + k_1 \chi_{(1,1)}(b) - \frac{3}{2} k_1 \chi_{(1,1)}(b) - \frac{3}{2} k_1 \chi_{(2)}(b) \end{aligned} \tag{7.33}$$

$$\begin{aligned} &= \frac{1}{2} (\chi_{(2)}(b) + \chi_{(1,1)}(b)) k_1^2 + \frac{1}{2} (\chi_{(2)}(b) - \chi_{(1,1)}(b)) \cdot (2 k_2) + \frac{1}{2} (\chi_{(2)}(b) - \chi_{(1,1)}(b)) k_1. \end{aligned} \tag{7.34}$$

Comparing this result with equation (7.24) concludes the proof of our claim.

Given the multiplicities in the decomposition of  $R$  into irreducible representations, we now can apply the theorem about the structure of the commutant from the previous

subsection. There exists some basis in which any matrix  $A \in \text{Com}(R)$  can be written as

$$A = \begin{pmatrix} M_{2 \times 2} & 0 & 0 & 0 & 0 \\ 0 & N_{2 \times 2} \otimes \mathbb{1}_{d-1} & 0 & 0 & 0 \\ 0 & 0 & u \mathbb{1}_{d-1} & 0 & 0 \\ 0 & 0 & 0 & v \mathbb{1}_{\frac{1}{2}(d-1)(d-2)} & 0 \\ 0 & 0 & 0 & 0 & w \mathbb{1}_{\frac{1}{2}d(d-3)} \end{pmatrix}, \quad (7.35)$$

where  $M_{2 \times 2}, N_{2 \times 2} \in \text{Mat}(2 \times 2, \mathbb{C})$  and  $u, v, w \in \mathbb{C}$ . Counting the free parameters in  $A$  we conclude that  $\text{Com}(R)$  is a

$$2 \cdot 2 + 2 \cdot 2 + 1 + 1 + 1 = 11 \quad (7.36)$$

dimensional, complex vector space. Moreover, we see from equation (7.35) that any matrix  $A^\dagger \in \text{Com}(R)^\dagger$  can be written as

$$A^\dagger = \begin{pmatrix} M_{2 \times 2}^\dagger & 0 & 0 & 0 & 0 \\ 0 & N_{2 \times 2}^\dagger \otimes \mathbb{1}_{d-1} & 0 & 0 & 0 \\ 0 & 0 & u \mathbb{1}_{d-1} & 0 & 0 \\ 0 & 0 & 0 & v \mathbb{1}_{\frac{1}{2}(d-1)(d-2)} & 0 \\ 0 & 0 & 0 & 0 & w \mathbb{1}_{\frac{1}{2}d(d-3)} \end{pmatrix}, \quad (7.37)$$

where this time the matrices  $M^\dagger$  and  $N^\dagger$  are hermitian  $2 \times 2$  matrices and the parameters  $u, v, w$  are real. Thus  $\text{Com}(R)^\dagger$  is an eleven dimensional, real vector space.



### 7.2.4 A basis for $\text{Com}(R)^\dagger$

**Theorem:** (Basis for  $\text{Com}(R)^\dagger$ ) *Let  $R$  be the representation defined in Subsection 7.2.1 and let  $d \geq 4$ . We write  $|e\rangle := \sum_i |i\rangle$ . The following list of matrices forms a basis for  $\text{Com}(R)^\dagger$ .*

$$\begin{aligned}
\mathcal{A}_1 &= \sum_i |i\rangle\langle i| \otimes \sum_j |j\rangle\langle j| = \mathbf{1} \otimes \mathbf{1} \\
\mathcal{A}_2 &= \sum_{i,j} |i\rangle\langle j| \otimes \sum_{i,j} |i\rangle\langle j| = |e\rangle\langle e| \otimes |e\rangle\langle e| \\
\mathcal{A}_3 &= \sum_i |i\rangle\langle i| \otimes \sum_{i,j} |i\rangle\langle j| + \sum_{i,j} |i\rangle\langle j| \otimes \sum_i |i\rangle\langle i| = \mathbf{1} \otimes |e\rangle\langle e| + |e\rangle\langle e| \otimes \mathbf{1} \\
\mathcal{A}_4 &= \sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle j| = d \Phi \\
\mathcal{A}_5 &= \sum_{i,j} |i\rangle\langle j| \otimes |j\rangle\langle i| = \mathcal{F} \\
\mathcal{A}_6 &= \sum_i |i\rangle\langle i| \otimes |i\rangle\langle i| = d T \\
\mathcal{A}_7 &= \sum_{i,j} |i\rangle\langle i| \otimes |i\rangle\langle j| + \sum_{i,j} |i\rangle\langle i| \otimes |j\rangle\langle i| + \sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle i| + \sum_{i,j} |j\rangle\langle i| \otimes |i\rangle\langle i| \\
\mathcal{A}_8 &= \sum_i |i\rangle\langle e| \otimes |i\rangle\langle e| + \sum_i |e\rangle\langle i| \otimes |e\rangle\langle i| \\
\mathcal{A}_9 &= \sum_i |e\rangle\langle i| \otimes |i\rangle\langle e| + \sum_i |i\rangle\langle e| \otimes |e\rangle\langle i| \\
\mathcal{A}_{10} &= i \left( \sum_{i,j} |i\rangle\langle i| \otimes |i\rangle\langle j| - \sum_{i,j} |i\rangle\langle i| \otimes |j\rangle\langle i| + \sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle i| - \sum_{i,j} |j\rangle\langle i| \otimes |i\rangle\langle i| \right) \\
\mathcal{A}_{11} &= i \left( \sum_i |i\rangle\langle e| \otimes |i\rangle\langle e| - \sum_i |e\rangle\langle i| \otimes |e\rangle\langle i| \right)
\end{aligned}$$

From the structure of the matrices it is evident, that they all are hermitian. Furthermore they are invariant under the conjugation with the swap operator. Therefore they are in the commutant of the representation  $S$  (see Subsection 7.2.1). Finally it is easy to see that each of the above matrices is invariant under conjugation with  $P \otimes P$  for any  $P \in \mathbb{P}$ . Hence, we conclude

$$\mathcal{A}_i \in \text{Com}(R)^\dagger \quad \forall i. \quad (7.38)$$

In the previous subsection we have already seen that the dimension of  $\text{Com}(R)^\dagger$  is 11. Thus if the matrices are linearly independent, we know that the list is complete. The linear independence is the only thing left to show to conclude the proof that the  $\{\mathcal{A}_i\}_{i \in \{1, \dots, 11\}}$  form a basis. For this we note that for any two hermitian matrices  $A$  and  $B$  we have the Schmidt scalar product  $\langle A|B \rangle = \text{tr}(A \cdot B)$ . We compute the Gramian matrix  $G$  whose entries are  $G_{ij} := \langle \mathcal{A}_j | \mathcal{A}_i \rangle$  for the Schmidt scalar product. This gives that

$$G = \begin{pmatrix} d^2 & d^2 & 2d^2 & d & d & d & 4d & 2d & 2d & 0 & 0 \\ d^2 & d^4 & 2d^3 & d^2 & d^2 & d & 4d^2 & 2d^3 & 2d^3 & 0 & 0 \\ 2d^2 & 2d^3 & 2d^2 + 2d^3 & 2d & 2d & 2d & 4d + 4d^2 & 4d^2 & 4d^2 & 0 & 0 \\ d & d^2 & 2d & d^2 & d & d & 4d & 2d^2 & 2d & 0 & 0 \\ d & d^2 & 2d & d & d^2 & d & 4d & 2d & 2d^2 & 0 & 0 \\ d & d & 2d & d & d & d & 4d & 2d & 2d & 0 & 0 \\ 4d & 4d^2 & 4d + 4d^2 & 4d & 4d & 4d & 12d + 4d^2 & 4d + 4d^2 & 4d + 4d^2 & 0 & 0 \\ 2d & 2d^3 & 4d^2 & 2d^2 & 2d & 2d & 4d + 4d^2 & 2d^2 + 2d^3 & 4d^2 & 0 & 0 \\ 2d & 2d^3 & 4d^2 & 2d & 2d^2 & 2d & 4d + 4d^2 & 4d^2 & 2d^2 + 2d^3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4d^2 - 4d & 4d^2 - 4d \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4d^2 - 4d & 2d^3 - 2d^2 \end{pmatrix}, \quad (7.39)$$

where  $d$  is the dimension of the vector space  $V$  and thus  $d^2$  is the dimension of the representation  $R$ . Later it will be useful to have  $G$  in block matrix form. We introduce the matrices  $G_1$  and  $G_2$  such that

$$G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix} \quad (7.40)$$

as above. (The zeros in the above matrix now correspond to matrices.) Inverting the matrices  $G_1$  and  $G_2$  depending on the dimension shows that

$$(G_1)^{-1} = \frac{1}{d(d-1)(d-2)(d-3)} \cdot \begin{pmatrix} d^2 - 3d + 1 & 1 & -d + 2 & 1 & 1 & -d^2 + d & d - 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -6 & 2 & -1 & -1 \\ -d + 2 & -1 & \frac{1}{2}(d-1) & -1 & -1 & 2d & -\frac{1}{2}(d+1) & 1 & 1 \\ 1 & 1 & -1 & d^2 - 3d + 1 & 1 & -d^2 + d & d - 1 & -d + 2 & -1 \\ 1 & 1 & -1 & 1 & d^2 - 3d + 1 & -d^2 + d & d - 1 & -1 & -d + 2 \\ -d^2 + d & -6 & 2d & -d^2 + d & -d^2 + d & d^3 + d^2 & -d^2 - d & 2d & 2d \\ d - 1 & 2 & -\frac{1}{2}(d+1) & d - 1 & d - 1 & -d^2 - d & \frac{1}{4}d^2 + \frac{1}{4}d + 1 & -\frac{1}{2}(d+1) & -\frac{1}{2}(d+1) \\ -1 & -1 & 1 & -d + 2 & -1 & 2d & -\frac{1}{2}(d+1) & \frac{1}{2}(d-1) & 1 \\ -1 & -1 & 1 & -1 & -d + 2 & 2d & -\frac{1}{2}(d+1) & 1 & \frac{1}{2}(d-1) \end{pmatrix} \quad (7.41)$$

and

$$(G_2)^{-1} = \frac{1}{d(d-1)(d-2)} \cdot \begin{pmatrix} \frac{d}{4} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \quad (7.42)$$

We conclude that the matrix  $G$  is invertible if and only if  $d \geq 4$ . The fact that the Gramian matrix of the list  $\{\mathcal{A}_i\}_{i \in \{1, \dots, 11\}}$  is invertible for  $d \geq 4$  implies that the list is linearly independent in this case. Then the list  $\{\mathcal{A}_i\}_{i \in \{1, \dots, 11\}}$  constitutes a basis of  $\text{Com}(R)^\dagger$ .

### 7.2.5 Evaluating the term $\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2}$

The previous subsections have shown that  $\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2}$  is an element of an 11-dimensional, real vector space. In addition the last subsection gave an explicit basis for that space. We now expand  $\sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2}$  into that basis. That is, we write

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} = \sum_j^{11} \alpha_j \mathcal{A}_j \quad (7.43)$$

with real coefficients  $\alpha_k$  depending on  $\mathcal{T}$ . We would like to have an explicit formula for the coefficients in terms of  $(\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E]$ . This can be achieved calculating

$$\text{tr} \left( \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} \cdot \mathcal{A}_k \right) = \sum_{P \in \mathbb{P}(A)} \text{tr} \left( (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot (P_A^\dagger)^{\otimes 2} \mathcal{A}_k (P_A)^{\otimes 2} \right) \quad (7.44)$$

$$= \sum_{P \in \mathbb{P}(A)} \text{tr} \left( (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot \mathcal{A}_k \right) \quad (7.45)$$

$$= |\mathbb{P}| \text{tr} \left( (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot \mathcal{A}_k \right). \quad (7.46)$$

Together with equation (7.43) this implies that

$$\text{tr} \left( (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot \mathcal{A}_k \right) = \sum_j^{11} \alpha_j \text{tr} (\mathcal{A}_j \mathcal{A}_k) \quad (7.47)$$

$$= \sum_j^{11} G_{kj} \alpha_j, \quad (7.48)$$

where  $G$  is the Gramian matrix of the Schmidt scalar product of the  $\mathcal{A}_k$  as in equation (7.39). In the previous subsection we already calculated the inverse of the Gramian matrix. We can use it to invert the above equation and to obtain the coefficients  $\alpha_k$ .

$$\alpha_j = \sum_k^{11} (G^{-1})_{jk} \text{tr} \left( (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot \mathcal{A}_k \right). \quad (7.49)$$

Finally we can write

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} (P_A)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A^\dagger)^{\otimes 2} = \sum_{i,j}^{11} (G^{-1})_{ij} \operatorname{tr} ((\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot \mathcal{A}_i) \mathcal{A}_j. \quad (7.50)$$

This is the core result of this section. The formula allows us to generally calculate terms of the type (7.3) and thus provides the possibility to obtain decoupling lemmata with permutation operators similar to the Decoupling Lemma of Section 2.1. Strictly speaking this is valid only in dimensions higher than 3 and a similar discussion is required to find such formulas in the case that  $d \in \{1, 2, 3\}$ . Evidently these cases are easier to treat since the basis vector  $\mathcal{A}_i$  can be “restricted” to lower dimensions. In quantum information theory typically we are concerned with systems of high dimension (as for example in the discussion of the heat bath in Chapter 3) we therefore will leave it with formula (7.50). Technically this formula is much more difficult to work with than its unitary counterpart equation (2.12). Instead of two linearly independent vectors that span the commutant algebra in the unitary case here we have eleven. Hence, formula (7.50) contains 121 terms (of which many are zero corresponding to the zero entries in the inverse Gramian matrix). This is the reason why we cannot just write down a decoupling theorem with an easy upper bound in terms of physical quantities. Instead, as already mentioned in the introduction to this chapter, we do the computations for three interesting special cases.

### 7.3 Distance from classicality

This section aims at answering the question, whether or not a map  $\mathcal{T}_{A \rightarrow E}$  can be made classicalizing with a pre concatenation of a permutation operator. We note that for a map  $\mathcal{T}_{A \rightarrow E}$  and its classicalized version  $\mathcal{T}_{A \rightarrow E}^{cl}$  one can write the Choi-Jamiolkowski representation of  $\mathcal{T}_{A \rightarrow E}^{cl}$  as (see (5.5))

$$\omega_{A'E}^{cl} = \mathcal{T}_{A \rightarrow E}^{cl}(\Phi_{AA'}) \quad (7.51)$$

$$= \mathcal{T}_{A \rightarrow E}(T_{AA'}), \quad (7.52)$$

For a fixed permutation operator  $P$  one can compare the Choi-Jamiolkowski representations of the map  $\mathcal{T}_{A \rightarrow E} \circ P \cdot$  and its classicalized version. If the distance of the two Choi-Jamiolkowski representations is measured in some norm (for example the Schatten 1-norm) this naturally implies a measure of distance on the set the corresponding maps: One can define the distance between two maps in some norm as being the distance of the Choi-Jamiolkowski representations. If we use the Schatten

1-norm on the state space the induced norm on the set of maps is the  $\Delta_{\text{PRO}}$  norm (see [6], Paragraph 4). With equation (7.52) (for  $d_{\text{R}} = d_{\text{A}}$ ) the term

$$\|\mathcal{T}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} (\Phi_{\text{AR}} - T_{\text{AR}}) P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}})\|_1$$

gives the distance between the Choi-Jamiolkowski representation of  $\mathcal{T}_{\text{A} \rightarrow \text{E}} \circ P \cdot$  and its classicalized version and can be interpreted as giving the  $\Delta_{\text{PRO}}$ -distance of the corresponding maps. Our result has applications especially in coding theory. We hope that it implies a classical one-shot coding theorem, similar to the quantum coding theorems presented in [5]. We follow equation (7.6) and have

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \|\mathcal{T}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} (\Phi_{\text{AR}} - T_{\text{AR}}) P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}})\|_2^2 \\ &= \text{tr} \left( (\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} ((P_{\text{A}}^{\dagger})^{\otimes 2} (\mathcal{T}^{\dagger})^{\otimes 2} [\mathcal{F}_{\text{E}}] (P_{\text{A}})^{\otimes 2}) \otimes \mathcal{F}_{\text{R}} \right) \end{aligned} \quad (7.53)$$

$$= \sum_{i,j}^{11} (G^{-1})_{ij} \text{tr} ((\mathcal{T}^{\dagger})^{\otimes 2} [\mathcal{F}_{\text{E}}] \cdot \mathcal{A}_i) \text{tr} ((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_{\text{R}}) \quad (7.54)$$

Of the 121 summands in the above sum many are zero. The inverse Gramian matrix  $G^{-1}$  has block diagonal structure (equation (7.40)). Hence any summand with  $(i, j) \in \{1, \dots, 9\} \times \{10, 11\}$  or  $(i, j) \in \{10, 11\} \times \{1, \dots, 9\}$  is zero. Therefore we can write

$$\sum_{i,j}^{11} (G^{-1})_{ij} \text{tr} ((\mathcal{T}^{\dagger})^{\otimes 2} [\mathcal{F}_{\text{E}}] \cdot \mathcal{A}_i) \text{tr} ((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_{\text{R}}) \quad (7.55)$$

$$\begin{aligned} &= \sum_{i,j}^9 (G^{-1})_{ij} \text{tr} ((\mathcal{T}^{\dagger})^{\otimes 2} [\mathcal{F}_{\text{E}}] \cdot \mathcal{A}_i) \text{tr} ((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_{\text{R}}) \\ &+ \sum_{i,j \in \{10, 11\}} (G^{-1})_{ij} \text{tr} ((\mathcal{T}^{\dagger})^{\otimes 2} [\mathcal{F}_{\text{E}}] \cdot \mathcal{A}_i) \text{tr} ((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_{\text{R}}). \end{aligned} \quad (7.56)$$

The operators  $\mathcal{A}_{10}$  and  $\mathcal{A}_{11}$  consist of a product of the imaginary unit and an anti-symmetric matrix. They engender the imaginary part of

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} (P_{\text{A}})^{\otimes 2} (\mathcal{T}^{\dagger})^{\otimes 2} [\mathcal{F}_{\text{E}}] (P_{\text{A}}^{\dagger})^{\otimes 2}.$$

Considering equation (7.6) it is evident that in our setup, where we calculate a norm (7.3) (and  $\lambda_{\text{AR}}$  is symmetric), these operators never can contribute. More precisely, for  $i, j \in \{10, 11\}$  the second trace term in the summands of (7.56),  $\text{tr} ((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_{\text{R}})$  is zero, because the trace of a product of a symmetric

and an antisymmetric matrix vanishes. Thus the operators  $\mathcal{A}_{10}$  and  $\mathcal{A}_{11}$  are irrelevant in our context. We stated them for completeness but, since we don't expect any contributions, after a blank line in Subsection 7.2.4. Moreover instead of working with the full Gramian matrix it suffices to work with  $(G_1)^{-1}$ , i. e.

$$\begin{aligned} & \sum_{i,j}^{11} (G_1^{-1})_{ij} \operatorname{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_i) \operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R) \\ &= \sum_{i,j}^9 (G_1^{-1})_{ij} \operatorname{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_i) \operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R). \end{aligned} \quad (7.57)$$

The terms  $\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R)$  can be calculated easily yielding

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_1 \otimes \mathcal{F}_R) = 0 \quad (7.58)$$

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_2 \otimes \mathcal{F}_R) = 1 - \frac{1}{d_R} \quad (7.59)$$

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_3 \otimes \mathcal{F}_R) = 0 \quad (7.60)$$

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_4 \otimes \mathcal{F}_R) = 0 \quad (7.61)$$

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_5 \otimes \mathcal{F}_R) = 1 - \frac{1}{d_R} \quad (7.62)$$

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_6 \otimes \mathcal{F}_R) = 0 \quad (7.63)$$

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_7 \otimes \mathcal{F}_R) = 0 \quad (7.64)$$

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_8 \otimes \mathcal{F}_R) = 0 \quad (7.65)$$

$$\operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_9 \otimes \mathcal{F}_R) = 2 \left(1 - \frac{1}{d_R}\right). \quad (7.66)$$

Equation (7.57) then becomes

$$\begin{aligned} & \sum_{i,j}^9 (G_1^{-1})_{ij} \operatorname{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_i) \operatorname{tr}((\Phi_{\text{AR}} - T_{\text{AR}})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R) \\ &= \left(1 - \frac{1}{d_R}\right) \sum_i^9 \operatorname{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_i) ((G_1^{-1})_{i2} + (G_1^{-1})_{i5} + 2(G_1^{-1})_{i9}) \end{aligned} \quad (7.67)$$

The matrix  $G_1^{-1}$  is known (7.41) and the terms  $(G_1^{-1})_{i2} + (G_1^{-1})_{i5} + 2(G_1^{-1})_{i9}$  are easily evaluated. We get

$$(G_1^{-1})_{12} + (G_1^{-1})_{15} + 2(G_1^{-1})_{19} = 0 \quad (7.68)$$

$$(G_1^{-1})_{22} + (G_1^{-1})_{25} + 2(G_1^{-1})_{29} = 0 \quad (7.69)$$

$$(G_1^{-1})_{32} + (G_1^{-1})_{35} + 2(G_1^{-1})_{39} = 0 \quad (7.70)$$

$$(G_1^{-1})_{42} + (G_1^{-1})_{45} + 2(G_1^{-1})_{49} = 0 \quad (7.71)$$

$$(G_1^{-1})_{52} + (G_1^{-1})_{55} + 2(G_1^{-1})_{59} = \frac{1}{d_A(d_A - 1)} \quad (7.72)$$

$$(G_1^{-1})_{62} + (G_1^{-1})_{65} + 2(G_1^{-1})_{69} = \frac{-1}{d_A(d_A - 1)} \quad (7.73)$$

$$(G_1^{-1})_{72} + (G_1^{-1})_{75} + 2(G_1^{-1})_{79} = 0 \quad (7.74)$$

$$(G_1^{-1})_{82} + (G_1^{-1})_{85} + 2(G_1^{-1})_{89} = 0 \quad (7.75)$$

$$(G_1^{-1})_{92} + (G_1^{-1})_{95} + 2(G_1^{-1})_{99} = 0 \quad (7.76)$$

and equation (7.67) becomes

$$\left(1 - \frac{1}{d_R}\right) \sum_i^9 \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_i) ((G_1^{-1})_{i2} + (G_1^{-1})_{i5} + 2(G_1^{-1})_{i9}) \quad (7.77)$$

$$= \frac{1}{d_R d_A} \frac{d_R - 1}{d_A - 1} (\text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_5) - \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_6)) \quad (7.78)$$

$$= \frac{1}{d_R d_A} \frac{d_R - 1}{d_A - 1} \left( \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \mathcal{F}_A) - \sum_i \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] (|i\rangle\langle i|_A \otimes |i\rangle\langle i|_{A'})) \right) \quad (7.79)$$

$$= \frac{1}{d_R d_A} \frac{d_R - 1}{d_A - 1} \left( \text{tr}(\mathcal{F}_E \mathcal{T}^{\otimes 2}(\mathcal{F}_A)) - \sum_i \text{tr}(\mathcal{T}(|i\rangle\langle i|_A) \mathcal{T}(|i\rangle\langle i|_{A'})) \right) \quad (7.80)$$

$$= \frac{1}{d_R d_A} \frac{d_R - 1}{d_A - 1} \left( d_A^2 \text{tr}(\mathcal{F}_E \text{tr}_{AA'}(\omega_{AE}^{\otimes 2}(\mathbb{1}_{EE'} \otimes \mathcal{F}_A))) - \sum_i \text{tr}(\mathcal{T}(|i\rangle\langle i|_A) \mathcal{T}(|i\rangle\langle i|_{A'})) \right) \quad (7.81)$$

$$= \frac{1}{d_R d_A} \frac{d_R - 1}{d_A - 1} \left( d_A^2 \text{tr}((\mathcal{F}_E \otimes \mathbb{1}_{AA'}) \omega_{A'E}^{\otimes 2}(\mathbb{1}_{EE'} \otimes \mathcal{F}_A)) - \sum_i \text{tr}(\mathcal{T}(|i\rangle\langle i|_A) \mathcal{T}(|i\rangle\langle i|_{A'})) \right) \quad (7.82)$$

$$= \frac{1}{d_R d_A} \frac{d_R - 1}{d_A - 1} \left( d_A^2 \text{tr}(\omega_{AE}^2) - \sum_i \text{tr}(\mathcal{T}(|i\rangle\langle i|_A) \mathcal{T}(|i\rangle\langle i|_{A'})) \right) \quad (7.83)$$

$$= \frac{1}{d_R d_A} \frac{d_R - 1}{d_A - 1} (d_A^2 \text{tr}(\omega_{A'E}^2) - d_A^2 \text{tr}((\omega_{A'E}^d)^2)). \quad (7.84)$$

Equation (7.80) uses the explicit form of the inverse of the Choi-Jamiolkowski isomorphism to express  $\mathcal{T}_{A \rightarrow E}$  via its Choi-Jamiolkowski representation (*Lemma 5* in [19]).

The last step (7.84) is by the definition of the Choi-Jamiolkowski representation of the classicalizing version of  $\mathcal{T}_{A \rightarrow E}$  and is shown in detail following equation (5.42). An easy reformulation can be used to see that

$$\text{tr}(\omega_{A'E}^2) - \text{tr}((\omega_{A'E}^{cl})^2) = \|\omega_{A'E} - \omega_{A'E}^{cl}\|_2^2. \quad (7.85)$$

We arrive at the following lemma.

**Lemma:** (Distance from classicality)

Introduce the states  $\Phi_{AR} := \frac{1}{d_R} \sum_{i,j} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_R$  and  $T_{AR} := \frac{1}{d_R} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_R$  with  $d_A \geq d_R$  and  $d_A \geq 4$ . Let  $\mathcal{T}_{A \rightarrow E} \in \text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$  be a linear map with Choi-Jamiolkowski representation  $\omega_{A'E} \in \mathcal{L}^\dagger(\mathcal{H}_E \otimes \mathcal{H}_{A'})$ , then

$$\begin{aligned} \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R (\Phi_{AR} - T_{AR}) P_A^\dagger \otimes \mathbb{1}_R) \right\|_2^2 \\ = \frac{d_A}{d_R} \frac{d_R - 1}{d_A - 1} \|\omega_{A'E} - \omega_{A'E}^{cl}\|_2^2, \end{aligned}$$

where the summation goes over all permutation operators.

Using the Hölder inequality (2.30) as in the previous chapters we obtain the following result.

**Theorem:** (Distance from classicality)

Introduce the states  $\Phi_{AR} := \frac{1}{d_R} \sum_{i,j} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_R$  and  $T_{AR} := \frac{1}{d_R} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_R$  with  $d_A \geq 4$ . Let  $\mathcal{T}_{A \rightarrow E} \in \text{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_E))$  be a completely positive map with Choi-Jamiolkowski representation  $\omega_{A'E} \in \mathcal{S}_\leq(\mathcal{H}_E \otimes \mathcal{H}_{A'})$ , then

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R (\Phi_{AR} - T_{AR}) P_A^\dagger \otimes \mathbb{1}_R) \right\|_1 \leq \sqrt{d_A \frac{d_R - 1}{d_A - 1}} 2^{-\frac{1}{2} H_2(A'|E)_\omega},$$

where the summation goes over all permutation operators.



## 7.4 Decoupling with permutations operators

We follow equation (7.6) and have

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R (\Phi_{AR} - \pi_{AR}) P_A^\dagger \otimes \mathbb{1}_R) \right\|_2^2 \\ &= \text{tr} \left( (\Phi_{AR} - \pi_{AR})^{\otimes 2} \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} ((P_A^\dagger)^{\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] (P_A)^{\otimes 2}) \otimes \mathcal{F}_R \right) \end{aligned} \quad (7.86)$$

$$= \sum_{i,j}^9 ((G_1)^{-1})_{ij} \text{tr} ((\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot \mathcal{A}_i) \text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R) \quad (7.87)$$

The last equation makes use of the same arguments as equation (7.57). Evaluating the terms  $\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R)$  this time yields

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_1 \otimes \mathcal{F}_R) = 0 \quad (7.88)$$

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_2 \otimes \mathcal{F}_R) = 1 - \frac{1}{d_R} \quad (7.89)$$

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_3 \otimes \mathcal{F}_R) = 0 \quad (7.90)$$

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_4 \otimes \mathcal{F}_R) = \frac{1}{d_R} \left( 1 - \frac{1}{d_R} \right) \quad (7.91)$$

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_5 \otimes \mathcal{F}_R) = 1 - \frac{1}{d_R^2} \quad (7.92)$$

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_6 \otimes \mathcal{F}_R) = \frac{1}{d_R} \left( 1 - \frac{1}{d_R} \right) \quad (7.93)$$

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_7 \otimes \mathcal{F}_R) = \frac{4}{d_R} \left( 1 - \frac{1}{d_R} \right) \quad (7.94)$$

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_8 \otimes \mathcal{F}_R) = \frac{2}{d_R} \left( 1 - \frac{1}{d_R} \right) \quad (7.95)$$

$$\text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_9 \otimes \mathcal{F}_R) = 2 \left( 1 - \frac{1}{d_R^2} \right). \quad (7.96)$$

Plugging all these terms into (7.87) gives:

$$\begin{aligned} & \sum_{i,j}^9 ((G_1)^{-1})_{ij} \text{tr} ((\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot \mathcal{A}_i) \text{tr} ((\Phi_{AR} - \pi_{AR})^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R) \\ &= \frac{1}{d_R} \left( 1 - \frac{1}{d_R} \right) \sum_i^9 \text{tr} ((\mathcal{T}^\dagger)^{\otimes 2} [\mathcal{F}_E] \cdot \mathcal{A}_i) \cdot \\ & \quad (d_R (G_1^{-1})_{i2} + (G_1^{-1})_{i4} + (d_R + 1)(G_1^{-1})_{i5} + (G_1^{-1})_{i6} + 4(G_1^{-1})_{i7} + 2(G_1^{-1})_{i8} + 2(d_R + 1)(G_1^{-1})_{i9}) \end{aligned} \quad (7.97)$$

The terms

$$(d_R (G_1^{-1})_{i2} + (G_1^{-1})_{i4} + (d_R + 1)(G_1^{-1})_{i5} + (G_1^{-1})_{i6} + 4(G_1^{-1})_{i7} + 2(G_1^{-1})_{i8} + 2(d_R + 1)(G_1^{-1})_{i9})$$

are easily computed using (7.41).

$$\begin{aligned} & (d_R(G_1^{-1})_{12} + (G_1^{-1})_{14} + (d_R + 1)(G_1^{-1})_{15} + (G_1^{-1})_{16} + 4(G_1^{-1})_{17} + 2(G_1^{-1})_{18} + 2(d_R + 1)(G_1^{-1})_{19}) \\ &= \frac{-1}{d_A(d_A - 1)} \end{aligned} \quad (7.98)$$

$$\begin{aligned} & (d_R(G_1^{-1})_{22} + (G_1^{-1})_{24} + (d_R + 1)(G_1^{-1})_{25} + (G_1^{-1})_{26} + 4(G_1^{-1})_{27} + 2(G_1^{-1})_{28} + 2(d_R + 1)(G_1^{-1})_{29}) \\ &= 0 \end{aligned} \quad (7.99)$$

$$\begin{aligned} & (d_R(G_1^{-1})_{32} + (G_1^{-1})_{34} + (d_R + 1)(G_1^{-1})_{35} + (G_1^{-1})_{36} + 4(G_1^{-1})_{37} + 2(G_1^{-1})_{38} + 2(d_R + 1)(G_1^{-1})_{39}) \\ &= 0 \end{aligned} \quad (7.100)$$

$$\begin{aligned} & (d_R(G_1^{-1})_{42} + (G_1^{-1})_{44} + (d_R + 1)(G_1^{-1})_{45} + (G_1^{-1})_{46} + 4(G_1^{-1})_{47} + 2(G_1^{-1})_{48} + 2(d_R + 1)(G_1^{-1})_{49}) \\ &= 0 \end{aligned} \quad (7.101)$$

$$\begin{aligned} & (d_R(G_1^{-1})_{52} + (G_1^{-1})_{54} + (d_R + 1)(G_1^{-1})_{55} + (G_1^{-1})_{56} + 4(G_1^{-1})_{57} + 2(G_1^{-1})_{58} + 2(d_R + 1)(G_1^{-1})_{59}) \\ &= \frac{d_R}{d_A(d_A - 1)} \end{aligned} \quad (7.102)$$

$$\begin{aligned} & (d_R(G_1^{-1})_{62} + (G_1^{-1})_{64} + (d_R + 1)(G_1^{-1})_{65} + (G_1^{-1})_{66} + 4(G_1^{-1})_{67} + 2(G_1^{-1})_{68} + 2(d_R + 1)(G_1^{-1})_{69}) \\ &= \left(1 - \frac{d_R}{d_A}\right) \frac{1}{d_A - 1} \end{aligned} \quad (7.103)$$

$$\begin{aligned} & (d_R(G_1^{-1})_{72} + (G_1^{-1})_{74} + (d_R + 1)(G_1^{-1})_{75} + (G_1^{-1})_{76} + 4(G_1^{-1})_{77} + 2(G_1^{-1})_{78} + 2(d_R + 1)(G_1^{-1})_{79}) \\ &= 0 \end{aligned} \quad (7.104)$$

$$\begin{aligned} & (d_R(G_1^{-1})_{82} + (G_1^{-1})_{84} + (d_R + 1)(G_1^{-1})_{85} + (G_1^{-1})_{86} + 4(G_1^{-1})_{87} + 2(G_1^{-1})_{88} + 2(d_R + 1)(G_1^{-1})_{89}) \\ &= 0 \end{aligned} \quad (7.105)$$

$$\begin{aligned} & (d_R(G_1^{-1})_{92} + (G_1^{-1})_{94} + (d_R + 1)(G_1^{-1})_{95} + (G_1^{-1})_{96} + 4(G_1^{-1})_{97} + 2(G_1^{-1})_{98} + 2(d_R + 1)(G_1^{-1})_{99}) \\ &= 0 \end{aligned} \quad (7.106)$$

Together with equation (7.97) the above implies that

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_A \otimes \mathbb{1}_R (\Phi_{AR} - \pi_{AR}) P_A^\dagger \otimes \mathbb{1}_R) \right\|_2^2 \\ &= \frac{1}{d_R^2} \frac{d_R - 1}{d_A - 1} \left( -\frac{1}{d_A} \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_1) + \frac{d_R}{d_A} \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_5) + \left(1 - \frac{d_R}{d_A}\right) \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_6) \right). \end{aligned} \quad (7.107)$$

The occurring trace terms are evaluated as always (see (7.84) for an example) and we get

$$\begin{aligned} & \frac{1}{d_R^2} \frac{d_R - 1}{d_A - 1} \left( -\frac{1}{d_A} \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_1) + \frac{d_R}{d_A} \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_5) + \left(1 - \frac{d_R}{d_A}\right) \text{tr}((\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_E] \cdot \mathcal{A}_6) \right) \\ &= \frac{d_A^2}{d_R^2} \frac{d_R - 1}{d_A - 1} \left( -\frac{1}{d_A} \text{tr}(\omega_E^2) + \frac{d_R}{d_A} \text{tr}(\omega_{A'E}^2) + \left(1 - \frac{d_R}{d_A}\right) \text{tr}((\omega_{A'E}^{cl})^2) \right). \end{aligned} \quad (7.108)$$

We formulate this result in a separate lemma:

**Lemma:** (Decoupling lemma for permutations)

Introduce the states  $\Phi_{\text{AR}} := \frac{1}{d_{\text{R}}} \sum_{i,j} |i\rangle\langle j|_{\text{A}} \otimes |i\rangle\langle j|_{\text{R}}$  and  $\pi_{\text{AR}} := \frac{1}{d_{\text{R}}^2} \sum_{i,j} |i\rangle\langle i|_{\text{A}} \otimes |j\rangle\langle j|_{\text{R}}$  with  $d_{\text{A}} \geq 4$ . Let  $\mathcal{T}_{\text{A} \rightarrow \text{E}} \in \text{Hom}(\mathcal{L}(\mathcal{H}_{\text{A}}), \mathcal{L}(\mathcal{H}_{\text{E}}))$  be a linear map with Choi-Jamolkowski representation  $\omega_{\text{A}'\text{E}} \in \mathcal{L}^{\dagger}(\mathcal{H}_{\text{E}} \otimes \mathcal{H}_{\text{A}'})$ , then

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \mathcal{T}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} \Phi_{\text{AR}} P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}}) - \omega_{\text{E}} \otimes \pi_{\text{R}} \right\|_2^2 \\ &= \frac{d_{\text{A}}^2 d_{\text{R}} - 1}{d_{\text{R}}^2 d_{\text{A}} - 1} \left( \frac{d_{\text{R}}}{d_{\text{A}}} \text{tr}(\omega_{\text{A}'\text{E}}^2) - \frac{1}{d_{\text{A}}} \text{tr}(\omega_{\text{E}}^2) + \left(1 - \frac{d_{\text{R}}}{d_{\text{A}}}\right) \text{tr}((\omega_{\text{A}'\text{E}}^{\text{cl}})^2) \right), \end{aligned}$$

where the summation goes over all permutation operators.

It is interesting to note that in the case  $d_{\text{R}} = d_{\text{A}}$  the comparison of this lemma with the Decoupling Lemma of Section 2.1 shows that averaging over all permutations gives the same result as averaging over all unitaries. In the case that the system  $AA'$  is in the fully entangled state for any fixed operation  $\mathcal{T}_{\text{A} \rightarrow \text{E}}$  applied to the system  $A$  there is a permutation operator that decouples well.

Leaving out the negative terms on the right hand side and using our standard procedure, the above lemma can trivially be transformed into a Decoupling Theorem with Permutation Operators.

## 7.5 Decoupling Quantum States with a Permutations followed by the Partial Trace<sup>1</sup>

In quantum cryptography the pivotal Hash-Lemma is used to extract randomness from a classical source that might be correlated with a quantum system hold by an adversary [17, 21]. The following Lemma generalizes the Hash-Lemma to the case where one wants to decouple a quantum system from a quantum adversary using classical operations only. It can be seen as an intermediate step between the crucial Fully Quantum Slepian Wolf Theorem [8] and the Hash Lemma. We write  $A = (A_1 A_2)$

---

<sup>1</sup>The results of this section were obtained in the week after the deadline of this Master project.

and we consider the Schatten 2-distance. As in Equation 7.6 we have that

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_2^2 \\ &= \text{tr} \left( (\rho_{AR} - \pi_A \otimes \rho_R)^{\otimes 2} \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} (P_A^{\otimes 2} (\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2}) P_A^{\otimes 2 \dagger}) \otimes \mathcal{F}_R \right) \end{aligned} \quad (7.109)$$

$$= \sum_{i,j}^9 (G^{-1})_{ij} \text{tr} (\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_i) \text{tr} ((\rho_{AR} - \pi_A \otimes \rho_R)^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R). \quad (7.110)$$

We compute the coefficients

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_1) = d_A d_{A_2} \quad (7.111)$$

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_2) = d_A^2 \quad (7.112)$$

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_3) = 2d_A d_{A_2} \quad (7.113)$$

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_4) = d_A \quad (7.114)$$

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_5) = \frac{1}{d_{A_2}} d_A^2 \quad (7.115)$$

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_6) = d_A \quad (7.116)$$

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_7) = 4d_A \quad (7.117)$$

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_8) = 2d_A \quad (7.118)$$

$$\text{tr}(\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_9) = \frac{2}{d_{A_2}} d_A^2. \quad (7.119)$$

For convenience we shortly write  $x := d_A(d_A - 1)(d_A - 2)(d_A - 3)$  and  $c = d_A(d_{A_1} - 1)(d_{A_2} - 1)$  and compute the numbers  $c_j := \sum_i^9 (G_1^{-1})_{ij} \text{tr} (\mathcal{F}_{A_1} \otimes \mathbb{1}_{A_2 A'_2} \cdot \mathcal{A}_i)$  using the given form of  $G^{-1}$ . We get

$$c_2 = \frac{c}{x} \quad (7.120)$$

$$c_3 = -\frac{c}{x} \quad (7.121)$$

$$c_4 = \frac{c}{x} \quad (7.122)$$

$$c_5 = \frac{d_A(d_{A_1} - 1)(d_A - 2)(d_A - 3) + c}{x} \quad (7.123)$$

$$c_6 = d_A(d_A - 5) \frac{c}{x} \quad (7.124)$$

$$c_7 = \frac{2c}{x} \quad (7.125)$$

$$c_8 = -\frac{c}{x} \quad (7.126)$$

$$c_9 = -\frac{c}{x} \quad (7.127)$$

and obtain that

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_2^2 \\ &= \sum_j^9 c_j \text{tr} \left( (\rho_{AR} - \pi_A \otimes \rho_R)^{\otimes 2} \mathcal{A}_j \otimes \mathcal{F}_R \right) \end{aligned} \quad (7.128)$$

$$\begin{aligned} &= \frac{d_{A_1} - 1}{d_A - 1} \text{tr} \left( (\rho_{AR} - \pi_A \otimes \rho_R)^{\otimes 2} \mathcal{A}_5 \otimes \mathcal{F}_R \right) \\ &+ \frac{c}{d_A(d_A - 1)} \text{tr} \left( (\rho_{AR} - \pi_A \otimes \rho_R)^{\otimes 2} \mathcal{A}_6 \otimes \mathcal{F}_R \right) \\ &+ \frac{c}{x} \text{tr} \left( (\rho_{AR} - \pi_A \otimes \rho_R)^{\otimes 2} \mathcal{Y} \otimes \mathcal{F}_R \right), \end{aligned} \quad (7.129)$$

where  $\mathcal{Y} = \mathcal{A}_1 + \mathcal{A}_2 - \mathcal{A}_3 + \mathcal{A}_4 + \mathcal{A}_5 - 6\mathcal{A}_6 + 2\mathcal{A}_7 - \mathcal{A}_8 - \mathcal{A}_9$ . The first two terms can be evaluated directly with an application of the swap trick noting that the classicalized version of the swap operator is  $\mathcal{A}_6$ . This gives

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_2^2 \\ &= \frac{d_{A_1} - 1}{d_A - 1} \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_2^2 \\ &+ \frac{c}{d_A(d_A - 1)} \left\| \rho_{AR}^{cl} - \pi_A \otimes \rho_R \right\|_2^2 \\ &+ \frac{c}{x} \text{tr} \left( (\rho_{AR} - \pi_A \otimes \rho_R)^{\otimes 2} \mathcal{Y} \otimes \mathcal{F}_R \right). \end{aligned} \quad (7.130)$$

To bound the third term we note that the vector  $\mathcal{Y}$  was chosen in a way such that it corresponds to a multiple of the second column of  $G_1^{-1}$ . We have that

$$\mathcal{Y} = \sum_i x ((G_1)_{i2})^{-1} \mathcal{A}_i. \quad (7.131)$$

On the other hand any element of the commutant can be written in the  $\mathcal{A}_i$  basis via

$$\mathcal{X} = \sum_{i,j} ((G_1)_{ij})^{-1} \text{tr}(\mathcal{X} \mathcal{A}_j) \mathcal{A}_i. \quad (7.132)$$

Comparing Equations (7.131) and (7.132) we conclude that

$$\text{tr}(\mathcal{Y} \mathcal{A}_j) = x \delta_{2j}, \quad (7.133)$$

which implies  $\text{tr}(\mathcal{Y}^2) = x$ . The third term of Equation (7.130) can be bounded as follows. We have that

$$\begin{aligned} & \frac{c}{x} \text{tr} \left( (\rho_{\text{AR}} - \pi_{\text{A}} \otimes \rho_{\text{R}})^{\otimes 2} \mathcal{Y} \otimes \mathcal{F}_{\text{R}} \right) \\ &= \frac{c}{x} \text{tr} \left( (\rho_{\text{AR}} - \pi_{\text{A}} \otimes \rho_{\text{R}}) \otimes \mathbb{1}_{\text{A}'} (\rho_{\text{A}'\text{R}} - \pi_{\text{A}'} \otimes \rho_{\text{R}}) \otimes \mathbb{1}_{\text{A}} \mathcal{Y} \otimes \mathbb{1}_{\text{R}} \right) \end{aligned} \quad (7.134)$$

$$\leq \frac{c}{x} \text{tr} \left( (\rho_{\text{AR}} - \pi_{\text{A}} \otimes \rho_{\text{R}})^2 \right) \sqrt{\text{tr}(\mathcal{Y}^2)} \quad (7.135)$$

$$= \frac{c}{\sqrt{x}} \|\rho_{\text{AR}} - \pi_{\text{A}} \otimes \rho_{\text{R}}\|_2^2 \quad (7.136)$$

To obtain the inequality we note that Equation (7.134) has the same structure as the right hand side of Equation (3.36) and can be bounded identically. Thus, Inequality (7.135) follows from the derivations of Section 3.4. We note that for  $d_{\text{A}} \geq 4$

$$\frac{d_{\text{A}}(d_{\text{A}_1} - 1)(d_{\text{A}_2} - 1)}{\sqrt{d_{\text{A}}(d_{\text{A}} - 1)(d_{\text{A}} - 2)(d_{\text{A}} - 3)}} \leq 1$$

holds. Using this and plugging in  $c$  and  $x$  and we find

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(\text{A})} \left\| \text{tr}_{\text{A}_2}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} \rho_{\text{AR}} P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}}) - \pi_{\text{A}_1} \otimes \rho_{\text{R}} \right\|_2^2 \\ & \leq \frac{d_{\text{A}_1} - 1}{d_{\text{A}} - 1} \|\rho_{\text{AR}} - \pi_{\text{A}} \otimes \rho_{\text{R}}\|_2^2 \end{aligned} \quad (7.137)$$

$$\begin{aligned} & + \frac{(d_{\text{A}_1} - 1)(d_{\text{A}_2} - 1)}{d_{\text{A}} - 1} \|\rho_{\text{AR}}^{\text{cl}} - \pi_{\text{A}} \otimes \rho_{\text{R}}\|_2^2 \\ & + \frac{d_{\text{A}}(d_{\text{A}_1} - 1)(d_{\text{A}_2} - 1)}{\sqrt{d_{\text{A}}(d_{\text{A}} - 1)(d_{\text{A}} - 2)(d_{\text{A}} - 3)}} \|\rho_{\text{AR}} - \pi_{\text{A}} \otimes \rho_{\text{R}}\|_2^2 \\ & \leq \frac{d_{\text{A}_1} - 1}{d_{\text{A}} - 1} \text{tr}[\rho_{\text{AR}}^2] + \frac{(d_{\text{A}_1} - 1)(d_{\text{A}_2} - 1)}{d_{\text{A}} - 1} \text{tr}[(\rho_{\text{AR}}^{\text{cl}})^2] + \text{tr}[\rho_{\text{AR}}^2]. \end{aligned} \quad (7.138)$$

This statement can be transformed into a decoupling theorem with the Schatten 1-norm with an application of the Hölder Inequality (2.30). We proceed as in Section 5.2, Equations (5.53)-(5.54) and introduce the positive definite and normalized operator  $\zeta_{\text{R}}$  writing

$$\begin{aligned} & \left\| \text{tr}_{\text{A}_2}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} \rho_{\text{AR}} P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}}) - \pi_{\text{A}_1} \otimes \rho_{\text{R}} \right\|_1 \\ & \leq \left\| (\pi_{\text{A}_1} \otimes \zeta_{\text{R}})^{-\frac{1}{4}} \left( \text{tr}_{\text{A}_2}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} \rho_{\text{AR}} P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}}) - \pi_{\text{A}_1} \otimes \rho_{\text{R}} \right) (\pi_{\text{A}_1} \otimes \zeta_{\text{R}})^{-\frac{1}{4}} \right\|_2 \end{aligned} \quad (7.139)$$

$$= \sqrt{d_{\text{A}_1}} \left\| \text{tr}_{\text{A}_2}(P_{\text{A}} \otimes \mathbb{1}_{\text{R}} \tilde{\rho}_{\text{AR}} P_{\text{A}}^{\dagger} \otimes \mathbb{1}_{\text{R}}) - \pi_{\text{A}_1} \otimes \tilde{\rho}_{\text{R}} \right\|_2 \quad (7.140)$$

To keep the notation simple we introduced an operator  $\tilde{\rho}_{AR} := (\mathbb{1}_A \otimes \zeta_R)^{-\frac{1}{4}} \rho_{AR} (\mathbb{1}_A \otimes \zeta_R)^{-\frac{1}{4}}$ . Thus, we can bound

$$\begin{aligned} & \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1^2 \\ & \leq \frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} d_{A_1} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \tilde{\rho}_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \tilde{\rho}_R \right\|_2^2 \end{aligned} \quad (7.141)$$

$$\leq d_{A_1} \left( \frac{d_{A_1} - 1}{d_A - 1} \text{tr}[\tilde{\rho}_{AR}^2] + \frac{(d_{A_1} - 1)(d_{A_2} - 1)}{d_A - 1} \text{tr}[(\tilde{\rho}_{AR}^{cl})^2] + \text{tr}[\tilde{\rho}_{AR}^2] \right), \quad (7.142)$$

where Inequality (7.142) uses (7.138). We now choose  $\zeta_R$  such that  $\text{tr}[\tilde{\rho}_{AR}^2]$  is minimal and we have  $\text{tr}[\tilde{\rho}_{AR}^2] \leq 2^{-H_{\min}(A|R)_\rho}$ . Furthermore note that by the definition of the min-entropy we have that

$$\rho_{AR} \leq 2^{-H_{\min}(A|R)_\rho} \mathbb{1}_A \otimes \zeta_R$$

which implies that

$$\rho_{AB}^{cl} \leq 2^{-H_{\min}(A|R)_\rho} \mathbb{1}_A \otimes \zeta_R$$

and therefore

$$\text{tr}[(\tilde{\rho}_{AR}^{cl})^2] \leq \text{tr}(\rho_{AR}) 2^{-H_{\min}(A|R)_\rho} \leq 2^{-H_{\min}(A|R)_\rho}.$$

With this we bound the right hand side of Inequality (7.142)

$$\begin{aligned} & d_{A_1} \left( \frac{d_{A_1} - 1}{d_A - 1} \text{tr}[\tilde{\rho}_{AR}^2] + \frac{(d_{A_1} - 1)(d_{A_2} - 1)}{d_A - 1} \text{tr}[(\tilde{\rho}_{AR}^{cl})^2] + \text{tr}[\tilde{\rho}_{AR}^2] \right) \\ & \leq d_{A_1} \left( \frac{d_{A_1} - 1}{d_A - 1} 2^{-H_{\min}(A|R)_\rho} + \frac{(d_{A_1} - 1)(d_{A_2} - 1)}{d_A - 1} 2^{-H_{\min}(A|R)_\rho} + 2^{-H_{\min}(A|R)_\rho} \right) \end{aligned} \quad (7.143)$$

$$\leq 2 \cdot d_{A_1} \cdot 2^{-H_{\min}(A|R)_\rho}. \quad (7.144)$$

**Theorem:** (Decoupling Quantum States with Classical Operations)

Let  $\rho_{AR} \in \mathcal{S}_{\leq}(\mathcal{H}_{AR})$  be a sub normalized density operator and let  $d_A \geq 4$ , then

$$\frac{1}{|\mathbb{P}|} \sum_{P \in \mathbb{P}(A)} \left\| \text{tr}_{A_2} (P_A \otimes \mathbb{1}_R \rho_{AR} P_A^\dagger \otimes \mathbb{1}_R) - \pi_{A_1} \otimes \rho_R \right\|_1 \leq \sqrt{2 d_{A_1} 2^{-H_{\min}(A|R)_\rho}},$$

where the summation goes over all permutation operators.

We note that the above formula generalizes the Hash Lemma obtained in Section 5.2. Furthermore it implies that there is a classical operation that decouples well in the sense of the lemma. The fully classical Hash Lemma contains essentially the same upper bound as the above and is known to be tight [17, 21]. Therefore one cannot expect significantly better bounds in the above formula. An extension of the above using approximate 2-wise independent families of permutations in the spirit of [21] can be obtained using the techniques developed in the previous chapters.



# Appendix A

## Hölder Inequality

We state Hölder inequality as given in [1]:

**Theorem:** (Hölder Inequality for Unitarily Invariant Norms) *For every unitarily invariant norm and for all square matrices  $A, B$*

$$\|AB\| \leq \| |A|^p \|_p^{\frac{1}{p}} \| |B|^q \|_q^{\frac{1}{q}}$$

*for all  $p > 1$  and  $\frac{1}{p} + \frac{1}{q} = 1$ .*

If one applies the inequality twice, one arrives at the following corollary.

**Corollary:** (Hölder Inequality for Three Matrices) *For every unitarily invariant norm and for all square matrices  $A, B, C$*

$$\|ABC\| \leq \| |A|^r \|_r^{\frac{1}{r}} \| |B|^s \|_s^{\frac{1}{s}} \| |C|^t \|_t^{\frac{1}{t}}$$

*for all  $r > 1$  and  $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} = 1$ .*

# Appendix B

## Jensen Inequality

For completeness we shortly state the widely used Jensen Inequality:

**Jensen Inequality:** *Let  $(\Omega, A, \mu)$  be a measure space, with  $\mu(\Omega) = 1$ . If  $g$  is a real-valued function that is  $\mu$ -integrable, and if  $\varphi$  is a convex function on the real numbers, then:*

$$\varphi\left(\int_{\Omega} g \, d\mu\right) \leq \int_{\Omega} \varphi \circ g \, d\mu.$$

Note that if  $\varphi$  is concave then  $-\varphi$  must be convex. Therefore the Jensen Inequality is also valid for concave functions  $\varphi$ , but with the inequality sign reversed. We will often use the Jensen Inequality for the concave square root.

# Appendix C

## Swap Trick

The Swap Trick is of crucial importance throughout the derivations in this thesis. For a fixed basis  $|i\rangle_A$  of some Hilbert space  $\mathcal{H}_A$  we introduce the swap operator  $\mathcal{F}_A$  acting on the bipartite Hilbert space  $\mathcal{H}_{AA'}$ ,

$$\mathcal{F}_A := \sum_{i,j} |i\rangle\langle j|_A \otimes |j\rangle\langle i|_{A'}. \quad (\text{C.1})$$

We generally leave out the index of the second subsystem writing  $\mathcal{F}_A$  since it is determined by the first one already.

**Lemma:** (Swap Trick) *Let  $M, N \in \mathcal{L}(\mathcal{H}_A)$  and let  $\mathcal{F}$  be the swap operator, then*

$$\text{tr}(MN) = \text{tr}((M \otimes N)\mathcal{F})$$

This result can be shown writing down  $M$  and  $N$  in the standard basis directly:

$M = \sum_{i,j} m_{ij} |i\rangle\langle j|$  and  $N = \sum_{k,l} n_{kl} |k\rangle\langle l|$ . Then,

$$\text{tr}((M \otimes N)\mathcal{F}) = \text{tr}\left(\sum_{i,j,k,l} m_{ij} n_{kl} |i\rangle\langle j| \otimes |k\rangle\langle l| \mathcal{F}\right) \quad (\text{C.2})$$

$$= \text{tr}\left(\sum_{i,j,k,l} m_{ij} n_{kl} |i\rangle\langle l| \otimes |k\rangle\langle j|\right) \quad (\text{C.3})$$

$$= \sum_{i,j} m_{ij} n_{ji} \quad (\text{C.4})$$

$$= \text{tr}(MN). \quad (\text{C.5})$$

# Appendix D

## The Murnaghan-Nakayama Rule

The Murnaghan-Nakayama rule provides a possibility to graphically construct the values of the characters of the irreducible representations of the symmetric group  $S_d$ . It is a recursive rule that gives  $\chi_\lambda((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$  for a given conjugacy class labeled with  $((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$  and an irreducible representation labeled with a partition  $\lambda$  of  $d$ . A *skew hook* is a connected part of a Young Diagram which does not contain any  $2 \times 2$  subset of cells



and that can be removed in a way such that the remaining boxes still form a smaller valid Young Diagram. For example the marked boxes in the following diagram form 4-hooks.



For a skew hook starting in the  $i$ -th row of a Young Diagram and ending in the  $j$ -th row, we call the number  $k = j - i$  the *length* of the hook and the number  $s = (-1)^k$  its sign. In our example the length of the first skew hook is two, while the second one has length one.

The Murnaghan-Nakayama rule states that to calculate  $\chi_\lambda((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$  for a partition  $\lambda = (\lambda_1, \dots, \lambda_n)$  one can proceed with the following recursion: Choose the cycle with greatest length in  $((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$ . In a first step draw all possible ways of removing a skew hook of the length of that cycle from the diagram corresponding to  $\lambda$  and write down  $s = (-1)^k$  for each possibility (if there is no such way the contribution is zero). Then for each obtained sub diagram draw all ways of removing a hook of length of the second from the right cycle in  $((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$

again writing down the sign of each resulting diagram but this time multiply it with the sing of the parent diagram. Do this over all the cycles in  $((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$ , such that in the end there are no boxes left anymore. The sum of all the numbers obtained in the last step is  $\chi_\lambda((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$ . A more detailed discussion of the Murnaghan-Nakayama rule can be found in [18].

## D.1 The Irreps of $R$

This section aims at giving a sketch of a proof of the relations

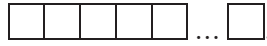
$$\chi_{(d)}(a) = 1 \tag{D.1}$$

$$\chi_{(d-1,1)}(a) = k_1 - 1 \tag{D.2}$$

$$\chi_{(d-2,1,1)}(a) = \frac{1}{2} (k_1 - 1)(k_1 - 2) - k_2 \tag{D.3}$$

$$\chi_{(d-2,2)}(a) = \frac{1}{2} k_1(k_1 - 3) + k_2 \tag{D.4}$$

which were used in Chapter 7. The first relation (D.1) is evident since the character of the trivial representation is one on any conjugacy class. Nevertheless we can use the Murnaghan-Nakayama rule to recover that value. The Young Diagram of the trivial representation of  $S_d$  has  $d$ -boxes arranged as



For a conjugacy class  $((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$  we pick the greatest cycle. There is only one possibility to erase a skew-hook from the above diagram in any case. For example if this cycle has length four this gives



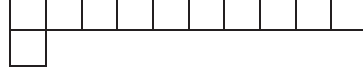
We note that the length of the skew hook is zero and its sign is  $+1$ . We then proceed to the next from the right cycle in the class  $((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d})$ . But again there is only one possibility to erase it and in any case the resulting sing is  $+1$ . This procedure can be done until no boxes are left anymore and the result is always

$$1 \cdot 1 \cdot 1 \cdot \dots \cdot 1 = 1, \tag{D.5}$$

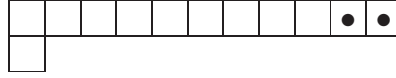
which proves (D.1).

We now consider (D.2) and do the calculation exemplary for  $S_{11}$ . The generalization

to  $S_d$  is straight forward. We fix some conjugacy class  $((1)^{k_1}, (2)^{k_2}, \dots, (11)^{k_{11}})$ . The Young Diagram corresponding to the irreducible representation is:



(In the general case there are  $d-1$  boxes in the upper row instead of ten.) Assume for now that  $k_1 \geq 2$ . For any cycle of length greater than one there is only one possibility to erase a skew hook from the diagram. For example for a two cycle we would get:



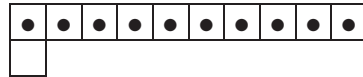
Since we assumed that  $k_1 \geq 2$  the sign will be  $+1$ . In this way it is possible to eliminate all cycles with length greater than one and the numerical value corresponding to the diagram will not change. The problem reduces to calculating the value of the resulting diagram with  $k_1 > 2$  boxes on a conjugacy class which contains  $k_1 \geq 2$  ones only. This time there are two possibilities to erase a box from the diagram and still to obtain a valid diagram. For example:



While the first diagram gives one immediately the second diagram again can be decomposed. The result is a summation: Each decomposition of a diagram into sub diagrams yields an additional one. Since one can decompose the diagram  $k_1 - 1$  times the sum is  $k_1 - 1$ . In total we have

$$\chi_{(10,1)}(((1)^{k_1}, (2)^{k_2}, \dots, (11)^{k_{11}})) = k_1 - 1 \quad (\text{D.6})$$

for  $k_1 \geq 2$ . The cases  $k_1 = 1$  and  $k_1 = 0$  we check explicitly. If  $k_1 = 1$  before we subtract the last box the situation is given by:



But the resulting diagram with the one box in the second row is not valid in any case so that the character is  $0 = 1 - 1$ . In the case  $k_1 = 0$  there is at least a two cycle at the end yielding to a skew hook of length one. The character in this case is

$$1 \cdot 1 \cdot \dots \cdot 1 \cdot (-1) = -1 \quad (\text{D.7})$$

$$= 0 - 1, \quad (\text{D.8})$$

which shows that the formula

$$\chi_{(10,1)} \left( ((1)^{k_1}, (2)^{k_2}, \dots, (11)^{k_{11}}) \right) = k_1 - 1 \quad (\text{D.9})$$

is valid in this cases, too. The reader should have no difficulties to see that the whole argumentation did not depend on  $d$ . Therefore

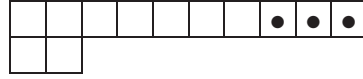
$$\chi_{(d-1,1)} \left( ((1)^{k_1}, (2)^{k_2}, \dots, (d)^{k_d}) \right) = k_1 - 1 \quad (\text{D.10})$$

and equation (D.2) is proved.

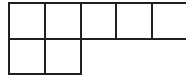
We proceed with the validation of (D.4):action of (D.4):

$$\chi_{(d-2,2)}(a) = \frac{1}{2} k_1(k_1 - 3) + k_2 \quad (\text{D.11})$$

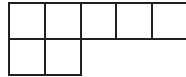
We start with considering the special case  $k_2 = 0$ , i. e. we evaluate the character on a conjugacy class that does not contain cycles of length two. As before, we do this exemplary for  $S_{12}$  (for notational convenience), but the generalization to arbitrary  $d$  is apparent. Assume for the moment  $k_1 \geq 4$ . As there are no two cycles in the conjugacy class by assumption the next shortest cycles after 1-cycles are three cycles. But there is only one possibility of subtracting skew hooks with three or more boxes from the diagram:



In any case the skew hook has sign one, such that the numerical value of the sub diagram always gets a factor of one from the parent diagram. After subtracting all skew hooks with more than one box we end up in a situation, where we have to evaluate a diagram of the type



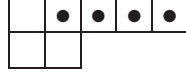
on a conjugacy class that contains  $k_1$  ones only. Since this is the conjugacy class of the identity the problem can equivalently be seen as the one of calculating the dimension of the irreducible representation



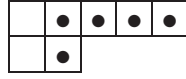
of  $S_{k_1}$ . This is done the easiest with an application of the Hook Formula [18]. The result is

$$\dim \left( \begin{array}{|c|c|c|c|c|} \hline \square & \square & \square & \square & \square \\ \hline \square & \square & & & \\ \hline \end{array} \right) = \frac{1}{2} k_1 (k_1 - 3).$$

Of course this result can also be obtained with an application of the Murnaghan-Nakayama rule. We check the cases  $k_1 \in \{1, 2, 3\}$  with explicit calculations. If  $k_1 = 3$ , then at the end there must be three boxes left but this is only possible if subtracts a skew hook in the following way:



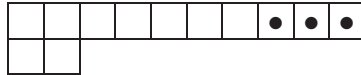
But the resulting diagram after the subtraction is not a valid Young Diagram and the result is therefore zero. If  $k_1 = 2$  at the end two boxes are left as for example in:



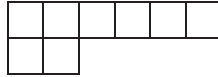
Note that in any case the drawn hook has sign  $-1$ , which adds an additional factor of  $-1$ . Thus in this case the result is  $-1$ . The case  $k_1 = 1$  yields the result  $-1$ . Finally in the case of  $k_1 = 0$  there is no possible valid skew hook that can fill all boxes at once and the result is zero. The formula

$$\chi_{(10,2)} \left( ((1)^{k_1}, (2)^0, \dots, (12)^{k_{12}}) \right) = \frac{1}{2} k_1 (k_1 - 3) \quad (\text{D.12})$$

is valid in any case. And again the argumentation shown is valid for general  $d$  which proofs (D.4) for all conjugacy classes that do not contain two cycles. We also need to consider that case to complete the proof. But even if there are 2-cycles, as before, there is only way of subtracting skew hooks with three or more boxes from the diagram:



The prefactor is always one and we are left with a situation, where we have to evaluate a character of the type



on a conjugacy class that contains 2- and 1-cycles only. For the moment again assume that  $k_1 \geq 4$ . There are generally two possibilities to remove a 2-hook from such a diagram:



The first one yields 1 in any case, while the second one can again be decomposed in the same manner until there are only  $k_1$  1-cycles left. Each decomposition adds a 1



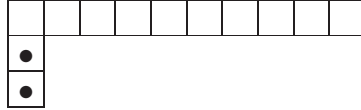
to the total sum, while the remaining diagram is of the type discussed above i. e. it can be treated with the formula

$$\chi_{(k_1-2,2)}(((1)^{k_1}, (2)^0, \dots, (12)^0)) = \frac{1}{2} k_1(k_1 - 3). \quad (\text{D.13})$$

Since there are  $k_2$  possible decompositions we obtain generalizing the above discussion to  $S_d$  that for  $k_1 \geq 4$

$$\chi_{(d-2,2)}(a) = \frac{1}{2} k_1(k_1 - 3) + k_2. \quad (\text{D.14})$$

The remaining cases can be checked by explicit calculations. Analogously one verifies formula (D.3). The only real difference is that in this case erasing a skew hook of the type



gives a  $-1$  instead of a  $+1$ .

# Bibliography

- [1] R. Bhatia. *Matrix Analysis*. Springer, 1996.
- [2] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285, 1975.
- [3] O. Dahlsten, R. Oliveira, and M. Plenia. Emergence of typical entanglement in two-party random processes. arXiv: 0701125v1 [quant-ph], 2007.
- [4] L. del Rio, J. Åberg, R. Renner, O. Dahlsten, and V. Vedral. The thermodynamic meaning of negative entropy. arXiv: 1009.1630v1 [quant-ph], 2010.
- [5] F. Dupuis. *The decoupling approach to quantum information theory*. PhD thesis, Université de Montréal, 2009.
- [6] A. Gilchrist, N. Langford, and M. Nielsen. Distance measures to compare real and ideal quantum processes. arXiv: 0408063v2 [quant-ph], 2009.
- [7] A. Harrow and R. Low. Random quantum circuits are approximate 2-designs. arXiv: 0802.1919v3 [quant-ph], 2009.
- [8] P. Hayden, A. Abeyesinghe, I. Devetak, and A. Winter. The mother of all protocols: Restructuring quantum information’s family tree. arXiv: 0606.225v1 [quant-ph], 2006.
- [9] P. Hayden and J. Preskill. Black holes as mirrors: quantum information in random subsystems. arXiv: 0708.4025v2 [quant-ph], 2007.
- [10] M. Horodecki, J. Oppenheim, and A. Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269(1):107–136, 2005.
- [11] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.

- [12] E. Kaplan, M. Naor, and O. Reingold. Derandomized construction of  $k$ -wise (almost) independent permutations. *Algorithmica*, 55:113–133, 2008.
- [13] M. Naor and O. Reingold. On the construction of pseudorandom permutations: Luby rackoff revisited. *Journal of Cryptology*, 12.1:29–66, 1997.
- [14] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [15] R. Renner. *Security of quantum key distribution*. PhD thesis, ETH Zürich, 2005. arXiv: 0403133 [quant-ph].
- [16] R. Renner. *Quantum Information Theory: Lecture Notes*. ETH Zürich, 2011.
- [17] R. Renner and R. König. Universally Composable Privacy Amplification Against Quantum Adversaries. In *Proc. TCC*, volume 3378 of *LNCS*, pages 407–425, Cambridge, USA, 2005. Springer.
- [18] B. E. Sagan. *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*. Springer: Graduate Texts in Mathematics, 2001.
- [19] O. Szehr. *The Decoupling Theorem: Semester Thesis*. ETH Zürich, 2010.
- [20] M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min- and max-entropies. arXiv: 0907.5238v2 [quant-ph], 2009.
- [21] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. arXiv: 1002.2436v1 [quant-ph], 2010.
- [22] J. Watrous. *Theory of Quantum Information: Lecture Notes*. University of Calgary, 2004.
- [23] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981.